NDoc Software Operations Manual

Third Party Software Information

For the purposes of disclosure, please note the following:

NDoc uses open source software **7-Zip** to compress certain files. **7-Zip** is licensed under the GNU LGPL license. For more information on **7-Zip**, please visit www.7-zip.org.

NDoc uses open source software NSIS to package certain executable files. NSIS is licensed under the zlib/libpng license. For more information on NSIS, please visit www.nsis.sourceforge.net.

Table of Contents

Overview

The Operations Manual provides a detailed account of the technical administration and operation of NDoc, including but not limited to installation and configuration procedures, security/authentication, and management of the Healthshare/Caché database platform.

In the Addendums, there is a section titled *Errors* with a listing of the more common NDoc errors and either steps to resolve or where to go to find possible workarounds.

Additional Documentation

Information regarding application requirements and planning for your implementation of NDoc can be found in the NDoc System Requirements Manual. Additional documentation for NDoc can be found at via the client resources of the website. This site contains many of our reference documents, FASTForms, release notes, training materials and technical guides that can provide additional details on various aspects of our software.

Access to the website is limited to specific individuals with credentials and should be requested in the Thornberry Help Center through the NDoc systems administrator for the agency

NDoc Support

- For any questions on this documentation or for NDoc assistance, please contact your System Manager to assist you and, if necessary, they can submit a support request via the Thornberry Help Center, which also contains articles for many commonly asked questions and issues.
- Emergency assistance is offered after normal business hours (M-F 8am-5:30pm) in case you have an NDoc issue requiring immediate assistance, such as system-wide access loss. You can reach Thornberry emergency support after hours via the Emergency Support Emergency Support Phone (Toll-free): (833) NDOC-911 OR (833) 636-2911

Security

This section provides guidance for clients to secure their external environment via their own toolsets and outlines the processes available in NDoc for providing PHI (Protected Health Information) security. Securing the environment is of utmost importance as today's expectations must be met for HIPAA compliance and privacy of all information. Confidentiality is a primary concern to any organization, patients and their families, and regulatory/accrediting bodies.

Additional websites providing guidance on this are:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

http://www.nist.gov/healthcare/security/hipaasecurity.cfm

Protecting your PHI

NDoc databases contain protected health information ("PHI"), and these databases are accessed in a variety of ways. This puts your agency at risk in at least two ways: the security of data at rest (i.e. stored in one or more NDoc databases) and the security of data in motion (i.e. data in transit between databases or between database and the data consumer).

Data at rest must be protected against unauthorized access due to theft or loss, by a combination of physical security/access control, firewalls and network security, login and password control, event logging/auditing, and timely installation of system patches.

Data in motion must be protected against eavesdropping and unauthorized access by encryption, hashing and using HTTPS for communications to the NDoc server.

In fact, any NDoc database access from a client device (or other system) over an open network, such as the Internet and wireless LANs, requires a secure connection due to transfer of PHI between requestor (or other system) and the NDoc database. HIPAA requires that PHI be protected on open networks against confidentiality failure, integrity failure and false remote nodes.

Encryption (making a plain text message into something unreadable) ensures the confidentiality (no unauthorized access) of the PHI. On NDoc standalone/local clients, an encryption solution is recommended which uses at least AES-256 256 bit encryption. VPNs connecting clients and server use AES-256 encryption.

Hashing (generating mathematically a value or values from a string of text) ensures the Integrity (no tampering with the data) of the PHI in motion and at rest. VPNs and SSL connecting clients and server use SHA1 hashing for protection against integrity failures.

SSL Tunneling with client and server certificate verification (using the Secure Socket Layer Protocol and the client's and server's certificate keys to identify each other) assures mutual authentication (no false nodes or "middle man" to intercept the data) for NDoc clients and/or other systems (lab system, hospital systems, HIEs, etc.). This ensures data is only transferred between trusted nodes.

Refer to the section *PHI Messaging with Confidentiality, Integrity, and Authentication* for more details on our protocols.

Areas to review

Server database (on-premise)

Whereas each customer is empowered to design a security solution appropriate for its business, data residing in a server database could be encrypted at the customer's discretion. A customer may decide and document their rationale, indicating physical security of the on-premise server is effective and sufficient to protect its on-premise server's data at rest. One requirement though is that you need to install an SSL certificate to your server which is outlined in the *Additional Requirements* section of the System Requirement Manual as communications are required to be through HTTPS.

Browsing to the on-premise server from a local (LAN) client

Customers with on-premise servers are responsible for implementing their own security solution for their direct connect devices. We do recommend that your internal communications be secure with only authorized personnel accessing your system with an authentication system in place. Additionally, configure your chosen web browser as described in the *Installation* section of this manual.

Browsing to the on-premise or hosted server from a remote (Internet) client

There are several potential reasons to access a remote NDoc database. You may have supervisors requiring database access from home during the evening or weekend hours; remote offices that use Internet connections to reach your NDoc server housed in a main office or data center. You may have field staff charting directly on the server over wireless Internet connections, rather than charting on a local database. For either of these scenarios, configure your chosen web browser as described in the Installation section of this manual.

Customers using the Thornberry hosted solution must utilize a provided secure remote desktop connection first before logging into NDoc. For more information please refer to the NDoc Hosted Solutions Manual located on our website under Welcome > Hosted Customers.

For customers using their own server, we recommend that communications should be directed over a VPN to utilize confidentiality, integrity and node authentication that VPN's provide.

Standalone/Local client database

We strongly recommend each standalone/local client be equipped with an NDoc database be encrypted. We recommend the use of an encryption program that has at least AES 256-bit encryption for the full drive. NDoc provides a security feature which closes out session access after a certain amount of inactivity. It is also recommended your agency standalone/local client devices be setup to logout of Windows after a period of inactivity as an additional layer of security but it should not cause the drive to sleep.

Synchronizing a standalone/local client database with a server database

Field staff often carry client devices containing NDoc databases containing PHI that must be securely synchronized with a host server. These synchronizations are file-based and protected during transfer between the standalone/local client and server with SFTP protocol.

Transmitting NDoc data to a third party

It is likely that your NDoc homecare/hospice patient data would be useful to another healthcare provider or other interested entity to support transitions of care or local, regional, national quality initiatives, etc. In fact, you may also become the recipient of other providers' patient information or wish to establish a lab results interface with a local hospital or reference lab.

You may send and receive batches of patient information, or a port may be opened through your firewall to enable TCP/IP-based data exchange. You must protect this connection against confidentiality and integrity failure, and provide mutual node authentication by using SSH, SSL, SFTP and/or VPN as you determine appropriate. Although the method and security of this data exchange is your agency's responsibility, Thornberry can help you implement appropriate technologies and safeguards to protect this data in motion. Refer to the section *PHI Messaging with Confidentiality, Integrity, and* Authentication for further details and contact us via the Thornberry Help Center to initiate a conversation.

Firewalls and network security

If your NDoc server is on-premise, putting NDoc data (and your users) behind a properly configured compliant firewall is your responsibility, and you will occasionally work with Thornberry representatives to create openings for data connections between your NDoc server and third party systems. If you are a hosted customer, your NDoc data is protected by a Cisco ASA 5505 firewall located in our SAS 70 Tier 3 data center.

Antivirus / Malware / Anti-Spyware

Computer viruses are a constant threat. Make sure to install and keep updated your software products dealing with these threats.

PHI Messaging with Confidentiality, Integrity, and Authentication

Intercommunication between NDoc and the wider world of external systems is becoming increasingly important. While NDoc supports a wide variety of communication protocols, there are three common goals in the protection of any Personal Health Information (PHI) over every protocol:

- Any PHI communicated shall be protected against confidentiality failures.
- Any PHI communicated shall be protected against integrity failures.
- Any PHI communicated shall be protected against false remote nodes.

Confidentiality is provided by encrypting the message content. The table below details which algorithm is used and how it is applied.

Integrity refers to ensuring that the entire message, header and data, has not been tampered with. A hash algorithm is calculated for the entire message.

False nodes are possible when a foreign server is inserted into the communication flow. These can be either client or server. Mutual Authentication is a method of ensuring that both client and server are legitimately authorized to communicate.

In the table below, functions, their descriptions and supported communication protocols are listed and the approach to encryption, integrity and mutual node authentication are described:

Protocol	**Encryption Used**	**Integrity**	**Mutual Authentication**
HTTPS	These interfaces can be configured to utilize SSL - 3DES or AES encryption between the NDoc server and the 3rd party.	SSL utilizes SHA1 hashing for protection against integrity failures.	SSL Server and Client Certificates that include Address Validation will provide mutual node authentication.
Feed, Service or Function Using HTTPS	**Description**		
Supervisory Access to EHR	Connection to NDoc required by evening/weekend on-call & supervisory personnel from their home		
Office employee access to EHR over LAN	Connecting local clients to the server		
Benchmarking	Export of patient data to vendors of homecare data benchmarking services		
Supplies	Import from a supply distributor of medical-surgical supplies shipped to a patient (or shipped to the agency on behalf of a patient)		
OASIS	Export of patient data to meet CMS requirements for standardized homecare data submission		
Orders	E-faxing of PDFs containing orders requiring physician signature		

Protocol	Encryption Used	Integrity	Mutual Authentication
SFTP	This interface utilizes this protocol in tandem with SSH and can be configured to utilize SSL - 3DES or AES encryption between the NDoc server and the 3rd party.	SSL utilizes SHA1 hashing for protection against integrity failures.	SSL Server and Client Certificates that include Address Validation will provide mutual node authentication.
Feed, Service or Function Using SFTP	**Description**		
Standalone/Local Database Synchronization	Connection between standalone/local client NDoc and server NDoc required to keep patient records and NDoc master files in sync		

Protocol	Encryption Used	Integrity	Mutual Authentication
HL7 2.x over TCP	These interfaces can be configured to utilize SSL - 3DES or AES encryption between the NDoc server and the 3rd party.	SSL utilizes SHA1 hashing for protection against integrity failures.	SSL Server and Client Certificates that include Address Validation will provide mutual node authentication.
Feed, Service or Function Using HL7 2. X over TCP	**Description**		
Patient Demographics	Export of key, non-clinical patient information to financial systems, HIEs and other healthcare providers		
Lab Results	Import of results generated from tests run on specimens delivered by agency personnel to a hospital or reference laboratory		

Protocol	Encryption Used	Integrity	Mutual Authentication
VPN	The VPN connection on the NDoc and third party servers will be configured to utilize either AES or 3DES VPN client and the database server.	SSL utilizes SHA1 hashing for protection against integrity failures.	SSL Server and Client Certificates that include Address Validation will provide mutual node authentication.
Feed, Service or Function Using VPN	**Description**		
Visits	Export of patient visit transactions to financial systems		

Protocol	Encryption Used	Integrity	Mutual Authentication
TCP	This interface can be configured to utilize SSL - 3DES or AES encryption between the NDoc server and the 3rd party.	SSL utilizes SHA1 hashing for protection against integrity failures.	SSL Server and Client Certificates that include Address Validation will provide mutual node authentication.
Feed, Service or Function Using TCPs	**Description**		
CAHPS	Export of patient data to meet the survey requirements of patient satisfaction vendors		
Patient Referrals	Import of key patient information from a referral source; intended to accelerate the intake process at the agency		
Patient Summary	Exchange of HITSP C32 Continuity of Care Documents with HIEs and other healthcare providers		

Securing your NDoc Environment

The following section reviews some of the methods of securing your NDoc environment. These can be discussed during implementation.

Managing Caché & HealthShare

NDoc utilizes a database platform created by InterSystems to hold all of the data entered. On the server, NDoc runs the HealthShare database platform. On clients, NDoc runs the Caché database platform. While HealthShare adds on top of Caché with capabilities for interfacing with other application providers, the overall database management remains the same.

IT Administrators of NDoc installations are required to manage the administrative passwords for each installation of NDoc, server or client. They are also responsible for setting up an account for Thornberry to use with full control over the database. Generally, we ask that no one make changes within the database without first consulting with Thornberry, but we do ask that you follow this procedure to setup an account that can be used by Thornberry for troubleshooting purposes.

Accessing System Management Portal

Caché and HealthShare use a web portal called the System Management Portal for managing the database with a graphical user interface. The database platform hosts an HTTP server on port 8972.

To access System Management Portal for a particular NDoc installation, follow these steps.

1. While on a desktop session of the machine in question, browse to System Management Portal (http://localhost:8972/csp/sys/UtilHome.csp)
2. Login with the SuperUser credentials created during installation (or any other user with the %All role)

Changing a Database User Password

When Caché and HealthShare are installed, all of the administrative accounts receive the same password. Although not necessary, InterSystems recommends making all of these passwords unique. The administrative users are

"SuperUser", "_SYSTEM", "Admin", and a user known as the "instance owner". The "instance owner" is named after the Windows account that installed NDoc and can be identified by its Full Name having the value "User who installed system".

Use this process to change the passwords of any database user:

1. Login to System Management Portal
2. Navigate to System Administration → Security → Users (http://localhost:8972/csp/sys/sec/%25CSP.UI.Portal.Users.zen)
3. Click on the name of the user you'd like to change the password for
4. Under "Password", select "Enter new password"
5. Enter and confirm a new random password
6. Click "Save" button

Creating a Database User for Troubleshooting by Thornberry

We ask that a persistent account be created on the server so we can easily access your server for day-to-day troubleshooting. Our technical staff will have access to the password as necessary for troubleshooting. For clients, we won't maintain the passwords given to us. Each time a technical support representative needs to access the database of a client device, we'll need to have a user setup and the credentials sent to us. The process for creating the user is the same on both install types, client and server.

1. Login to System Management Portal
2. Navigate to System Administration → Security → Users
3. Create or update user
    a. If a user named "Thornberry" already exist, change the password as described in the section above.
    b. Otherwise
        i. Click "Create New User" button
        ii. Enter the following details:
            1. Name: Thornberry
            2. Copy from: SuperUser
            3. Full Name: Thornberry Technical Support
            4. Password: *create a random password*
            5. Password (confirm): *confirm password*
        iii. Click "Save" button

Additional Resources

Documentation from InterSystems on all aspects of the database platform are available online at http://docs.intersystem.com/. A few direct links are provided here as well to help jump start learning how to manage your NDoc installations.

Caché 2016.1

- Documentation Home - http://docs.intersystems.com/cache20161/csp/docbook/DocBook.UI.Page.cls
- Glossary - http://docs.intersystems.com/cache20161/csp/docbook/DocBook.UI.Page.cls?KEY=RGOT_complete
- Security Administration: Users - http://docs.intersystems.com/cache20161/csp/docbook/DocBook.UI.Page.cls?KEY=GCAS_users

Default Database User Accounts

Both the InterSystems database platform and Thornberry's NDoc application create default users used for a variety of purposes. The following table will show all users that are created by default, who creates them, and what they are used for.

Username	Created By	Access Level	Description
SuperUser	InterSystems	Full Access	System Super user; Should be considered a "root" user
Admin	InterSystems	Manager	System Administrator
_SYSTEM	InterSystems	Full Access	SQL System Manager; Should be considered a "root" user
InstanceOwner	InterSystems	Full Access	User who installed system; Should be considered a "root" user; Can be deleted
CSPSystem	InterSystems	CSP Gateway	Only used for the CSP Gateway in the built-in Apache server to connect into the database.
UnknownUser	InterSystems	None	Only used for the WebLink Gateway in IIS to connect into the database.
_Ensemble	InterSystems	Full Access	Ensemble Manager; Should be considered a "root" user
_PUBLIC	InterSystems	None	Not a logon user. Holds the default Roles for new users.
ServerAdmin	Thornberry	Full Access	Server-Only; Administrative Account generated w/ random password
ClientAdmin	Thornberry	Full Access	Client-Only; Administrative Account generated w/ password available on the server
LogiReports	Thornberry	Full Access	*DEPRECATED*. Only used for LogiReports (our internal reporting engine) to make an ODBC connection into the database
NDocSynchronization	Thornberry	Read/Write for All NDoc DBs	*DEPRECATED*. Only used during the synchronization process

DeepSee_*CUSTOMER*	Thornberry	Read Only for CUSTOMER DBs	Only used for WebLink to create a session into DeepSee
*CUSTOMER*ODBC	Thornberry	Read Only for CUSTOMER DBs	Used for customers to setup their own ODBC-based reporting
*CUSTOMER*_SYNC	Thornberry	Read/Write for CUSTOMER DBs	Only used during the synchronization/refresh process
HHG_*CUSTOMER*	Thornberry	Read Only for CUSTOMER DBs	(Must have Home Health Gold) Only used by HHG to make an ODBC connection into the database

Encrypting your standalone/local client data

Securing your data while at rest is something we strongly advise you to do. Encryption offers one of the most secure ways to protect PHI if theft or loss occurs. Select a product using AES or variants thereof which provide 256-bit encryption and passwords are hashed with algorithms including SHA-512, RIPMED-160, etc. Other features to look for:

Creates a virtual encrypted disk within a file and mount it as a real disk.

Encrypts an entire partition or storage device such as USB flash drive or hard drive.

Encrypts a partition or drive where Windows is installed (pre-boot authentication).

Encryption is automatic, real-time (on-the-fly) and transparent.

Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.

Encryption can be hardware-accelerated on modern processors.

Using Antivirus/Malware/Anti-Spyware Software

All NDoc updates and patches are scanned with a commercial antivirus/malware application using the latest definitions prior to release. Thornberry's development and hosted environments are also constantly monitored and routinely scanned for viruses and malware.

NDoc works with most COTS antivirus/malware programs. We recommend that these packages be run at the server and client device level. Refer to our System Requirement Manual for any antivirus programs that we might have issues with at this point in time.

Starting with version 17.01, the way that we build certain executables has been shown to cause false positives with some anti-virus programs, and as such, necessary files have been quarantined or removed. To prevent this, we recommend putting the following exclusions in place:

- For servers - \ndoc\ and all subdirectories (the drive will be dependent on your configuration)
- For clients - C:\Ndoc\, c:\comm\ and all subdirectories of both

Server with NDoc installed

Due to the nature of how the Caché database operates, certain applications can degrade performance or cause clients to disconnect. Applications that monitor or throttle network connections need to be configured as to allow clients to connect. The following files should be excluded in antivirus and IDS scans. Scanning these files while the system is in use can degrade performance.

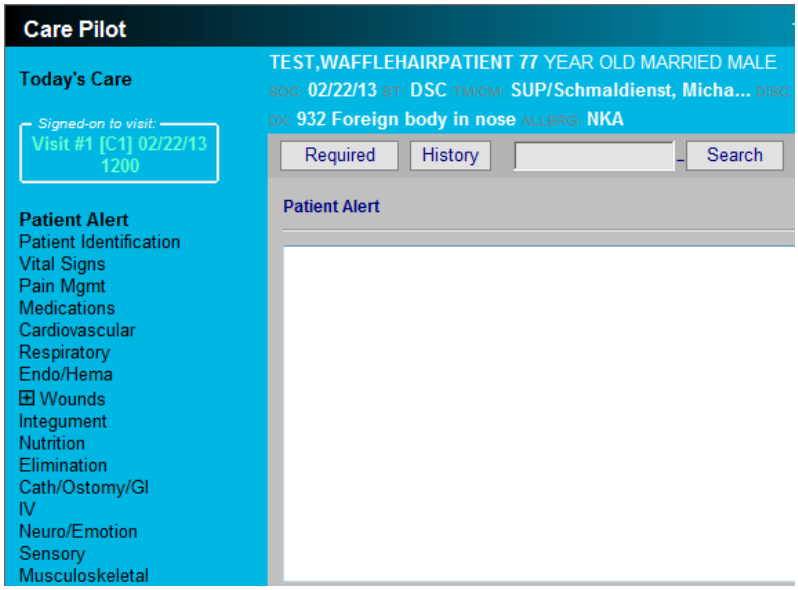
- \NDoc\cache.dat
- \NDoc\Agencies\<SITENAME>\audit\cache.dat
- \NDoc\Agencies\<SITENAME>\patient\cache.dat
- \NDoc\Agencies\<SITENAME>\cache.dat
- \NDoc\lib\cache.dat
- \NDoc\lib\fdb\cache.dat
- \NDoc\temp\cache.dat
- \NDoc\Intersystems\mgr\cache.dat
- \NDoc\Intersystems\mgr\cachelib\cache.dat
- \NDoc\Intersystems\mgr\cachetemp\cache.dat
- \NDoc\Intersystems\mgr\ensemble\cache.dat
- \NDoc\Intersystems\mgr\enslib\cache.dat
- \NDoc\Intersystems\mgr\cache.wij

Auditing NDoc transactions

We have several functions and reports available to view what has occurred in NDoc from both a clinical and security point of view. All of the functions/reports are available for the System Manager user type. The security audit, in two parts called Auditing Settings and Audited Events, is available for the Security Manager. Your system manager may grant other user types access to functions/reports at his/her discretion.

Field History

In certain functions like Care Pilot > Patient Profile or when charting a Visit one can view the history of individual fields. You would move your cursor to that field and click History (as shown to the right).

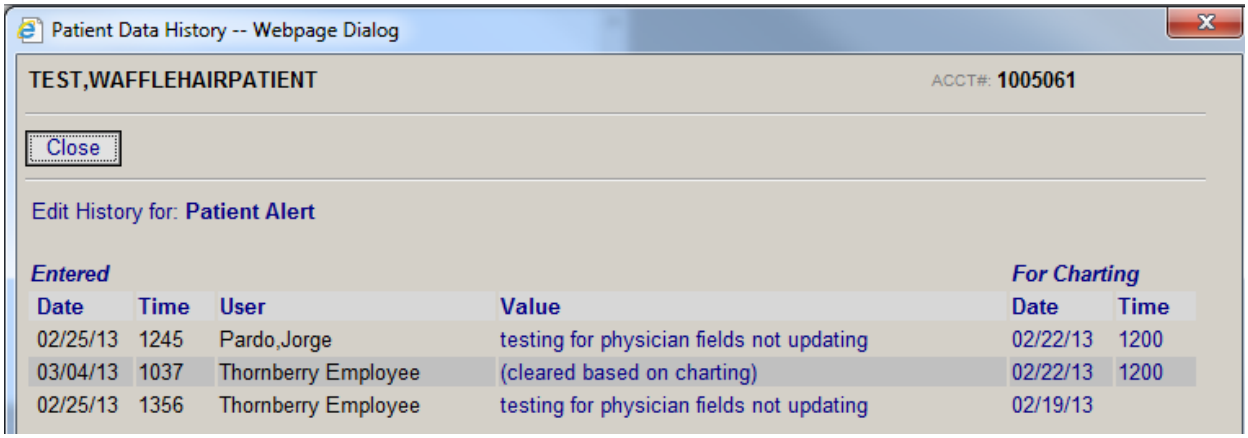


What displays is shown below. It contains the date/time the change was made, who made the change, what the values were, and in the For Charting column, lets you know where the change was made:

Referral - contains no date/time

Patient Profile - has just a date

Visit - has both date and time



Auditing Settings

Security auditing contains two components: the Audit Settings page detailed here and the Audited Events report detailed in the next section.

NDoc audits all attempts to access the application and the PHI stored within its database, as well as other key security-related events. These are collectively referred to as "audited events". Your Security Manager can review these events at any time, without viewing PHI, as a means to monitor the NDoc application for breaches of security and proper access to patient information. You also have the ability to manually export the audit logs for certain days, as detailed on the next page. Only the System Manager or Security Manager should have access to the Audit Settings page.

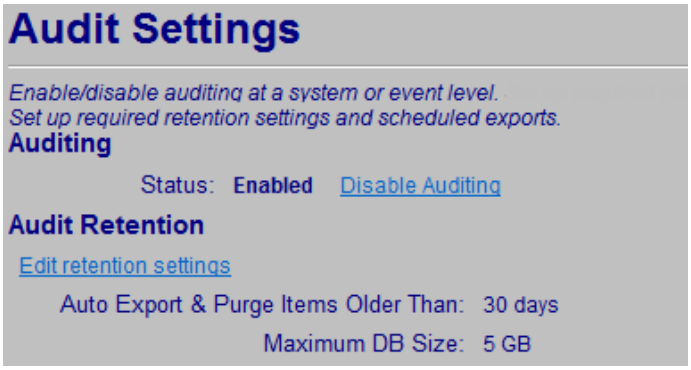
For Thornberry Cloud Services (hosted) customers, all audit settings are controlled by Thornberry and access is not provided to the end-users. All audited events are recorded are retained indefinitely. Customers may request access to audited events that have been exported and are no longer directly accessible in NDoc. The default is to retain 1825 days (5yrs) of audited events and to purge after reaching a maximum DB size of 5GB.

Accessing this page

Administration > System > Settings > Audit

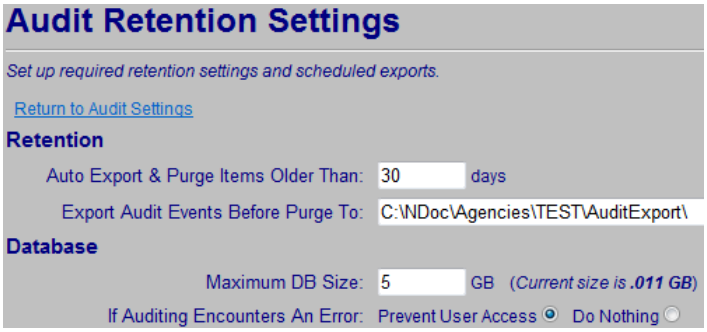
Modifying the settings

You can change a variety of settings from disabling auditing to selecting which areas you want to audit.



Auditing – The default is enabled. You can turn on/off auditing by clicking the Enable Auditing or Disable Auditing, though it is highly recommended that you do not disable this feature.

Audit Retention – The installation default is to retain 1825 days (5 yrs) of audited events and to purge after reaching a maximum DB size of 5 GB. Click on Edit Retention settings (screen shown below) to adjust your values:



- **Retention > Auto Export and Purge Items older than XX Days**: This is the number of days of auditing you want to maintain in your database before the system purges the entries by exporting them to a CSV file. There is no maximum, but the more days you keep, the larger the data storage required. The default is 1825 days (5yrs).
- **Retention > Export Audit Events Before Purge To**: This is the default path to store the CSV files, before the DB is purged. You can modify the path where you want to store the files.
- **Database > Maximum DB Size:** The default is 5 GB and is the minimum value that can be entered. Depending on the amount of staff and amount of work done, this might need to be set higher for your agency. You can also monitor the current size of the Audit Log to determine whether you need to increase the Maximum DB Size or Decrease the number of days for Auto Export and Purge to help save drive space or prevent errors from occurring.

- **If Auditing Encounters an Error**: This controls whether you want to allow NDoc users entry into the system while auditing is erroring (usually associated with can't write to the DB due to maximum size or the drive is full). Due to the fact that auditing might be important to your organization we, by default, install NDoc with Prevent User Access enabled. However, you may elect to have the system ignore the erroring and allow users access to the system by choosing Do Nothing. This selection allows user access, but user actions are not audited. The default is Prevent User Access.

Auditable events: The default is Enabled (marked Yes) for all events. You have the ability to customize which events you want audited. Click the Change Status button to have an event be Yes or No for Enabled. Once you change the status you can click Reload at the bottom of the list to refresh them. Refer to the section *Audit Trigger Events* for more details on what these cover.

Auditable Events

Event Name	Enabled	
System\Security\Audit_Change	Yes	Change Status
System\Security\Audit_Start	Yes	Change Status
System\Security\Audit_Stop	Yes	Change Status
System\Security\Start	Yes	Change Status
System\Security\Stop	Yes	Change Status
System\System\Backup	Yes	Change Status
System\System\Restore	Yes	Change Status
Application\Data\Med_Create	Yes	Change Status
Application\Data\Med_Update	Yes	Change Status
Application\Data\Order_Create	Yes	Change Status
Application\Data\Order_Update	Yes	Change Status
Application\Data\PHI_Export	Yes	Change Status
Application\Data\Patient_Create	Yes	Change Status
Application\Data\Patient_Query	Yes	Change Status
Application\Data\Patient_Update	Yes	Change Status
Application\Data\Patient_View	Yes	Change Status
Application\Data\Query	Yes	Change Status
Application\Data\Signature_Create	Yes	Change Status
Application\Login\Login	Yes	Change Status
Application\Login\Logout	Yes	Change Status
Application\Login\Node_Authenticate	Yes	Change Status
Application\Login\Terminate	Yes	Change Status
Application\Login\Timeout	Yes	Change Status
Application\Scheduling\Event_Create	Yes	Change Status
Application\Scheduling\Event_Delete	Yes	Change Status
Application\Scheduling\Event_Update	Yes	Change Status
Application\Security\Audit_Export	Yes	Change Status
Application\Security\Audit_Purge	Yes	Change Status
Application\Security\Patient_Assignment	Yes	Change Status
Application\Security\Setting_Change	Yes	Change Status
Application\Security\UserType_Create	Yes	Change Status
Application\Security\UserType_Update	Yes	Change Status
Application\Security\User_Create	Yes	Change Status
Application\Security\User_Update	Yes	Change Status
Interface\Data\PHI_Export	Yes	Change Status
Interface\Data\PHI_Import	Yes	Change Status
Interface\Data\Query	Yes	Change Status

Informational reports available

Several reports are available to review for troubleshooting and monitoring purposes. These provide another level of security knowing who has accessed your data and how, but can also be used to troubleshoot NDoc issues. Note that only events within the scope of NDoc are audited. For example, Windows logs should be investigated for information pertaining to Windows-specific activity; NDoc audits HealthShare but does not audit Windows backups.

Admin History

To access this report go to Reports > Auditing > Administrative History.

The Admin History report shows the history of table or routine changes within one or more NDoc functions for a range of dates. You can also view 485 History from here. The prompts are:

- From/Thru Date – includes changes on and between the 2 dates chosen.
- NDoc function – corresponding to the function as it is called in NDoc, you can choose one or more using the Shift or CTRL buttons to select multiple functions.

The report depending on the function chosen, displays the function, the device ID the change came from, the date/time, the user, the patient ID if appropriate, the field name and the older and newer values of the fields.

Audited Events

To access this report go to Reports > Auditing > Audited Events.

In the section *Auditing Settings*, you were shown where in Administration you can set up what is being audited. The Audited Events report details several actions occurring on the NDoc system when accessing the system and/or a patient. IT DOES NOT SHOW PHI, but does allow viewing a patient (via Account #) an employee accessed. The prompts are:

- Patient Account #(s): Separate with commas
- From - Thru Date/Time: Includes changes on and between the 2 dates/times chosen.
  NOTE: Per regulations time is in UTC so for EDT (UTC is 4 hours ahead)
- Component: Defaults to ALL. These are the major functions in NDoc.
- Event Type – Defaults to ALL. These represent specific component areas such as all Logins.
- Event Name: Defaults to ALL. These are events by name such as Audit Changes.
- User ID: Defaults to ALL. These are the User IDs that users login in with.
- Device: Defaults to ALL. These are the Device IDs of client devices
- Order: By default, the report lists events in chronological order (in ascending Date/Time sequence). You can choose a different ordering if needed.

User Activity by Device

To access this report go to Reports > Auditing > User Activity.

This report allows viewing of general functionality across any device for a range of dates by user(s) or patient. Use this report for a general understanding of what activity occurred with a patient or an employee through the day. The prompts are:

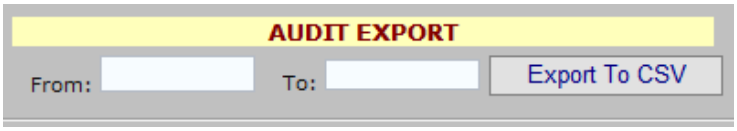
- From/Thru Date - includes changes on and between the 2 dates chosen.
- Device # - review by client device ID.
- Clinician – review by employee
- Event – specific events within functions (allows more granular detail if needed.
- Function – specific function in NDoc you can review.
- Patient – allows you to search for patient specific activity

Synchronization Report

To access this report go to Reports > Auditing > Synchronization Report. This report is available to understand what is happening with communications between the standalone/local clients and the NDoc server for a range of days and can be specific to certain standalone/local clients or employees. This allows troubleshooting issues with syncing which is the method that a standalone/local clients transfers visit/charting data, employee activity, etc. back and forth from the server.

- Date Range – select the dates that you want to view. The more days included, the longer the report takes to generate.
- Type of connections – defaults to ALL, but allows you to view specific connection types (direct, remote, etc).
- Standalone/Local Client IDs – View all standalone/local clients (default) or specific client IDs.
- Employee(s) – defaults to ALL employees or view just specific users.

Exporting audit logs



You have the ability to export audit logs for a number of days to a CSV file for reference and review. Access this function in Administration > System > Dashboard > located under Audit Export. Provide the day from and the day to (can be the same day) and click Export to CSV. The default time is 00:00 to 23:59 in UTC time. You then provide a path where to store the file. A sample of the output is below and it matches the Audited Events report if run at its default date/time.

```
Event Time,User ID,Machine ID,Component,Event Type,Event Name,Description,Patient ID,Outcome
"2013-03-27 06:00:27.091","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1003138",Success,""
"2013-03-27 06:01:15.742","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004218",Success,""
"2013-03-27 06:01:47.962","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004401",Success,""
"2013-03-27 06:02:45.364","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004416",Success,""
"2013-03-27 06:03:17.639","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004612",Success,""
"2013-03-27 06:03:54.978","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004625",Success,""
"2013-03-27 06:04:27.206","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004629",Success,""
"2013-03-27 06:04:59.652","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004633",Success,""
"2013-03-27 06:05:32.098","SYSTEM","SERVER:TEST","Interface","Data","PHI_Export","PHI exported via CCD Export","1004635",Success,""
```

Updating NDoc and its required components

There are three major "layers" comprising the NDoc infrastructure: Windows Operating Systems (OS), Caché/HealthShare (database environment from InterSystems Corp.), and the NDoc application itself. Each layer, consisting of executables and settings/persistent data, needs to be upgraded from time to time.

Windows

Supported Windows OS's are not included with your NDoc license but are required for Caché and NDoc operation. If NDoc is on the client's server, management and maintenance of the Windows OS and environment is your agency's responsibility. If you use Thornberry's server hosting service, Windows management is the responsibility of Thornberry and its Tier 3, SSAE-16 SOC 2 certified data center personnel.

Thornberry does not automatically ensure compatibility with released patches for supported OS's. Should an NDoc issue arise with an installed OS patch, contact Thornberry immediately via a request through the Thornberry Help Center. Your options then are to use the OS feature for uninstalling patches or if unable to uninstall for technical reasons, a system restore and perhaps determine if there is another way to protect against the attack (e.g. disabling services, enabling specific firewall rules, etc.) OR if you keep the patch, use your disaster recovery plan (e.g. working from paper) to continue day to day activities until Thornberry creates an NDoc patch allowing compatibility.

Thornberry recommends its customers use Windows Software Update Services ("WSUS") to manage their Windows patch process. For more information on WSUS see HTTPS://technet.microsoft.com/en-us/windowsserver/bb332157.aspx.

Caché

The database layer, Caché, is fairly static. Caché is the most widely used database in healthcare the world over and is renowned for its reliability, integrity and performance. This translates into a long "shelf life" for any particular version of Caché on which NDoc is installed and supported.

Approximately every 2-3 years you are asked to permit Thornberry personnel to "take your server down" for a 4-6 hour database upgrade. This applies to both on premise and hosting situations. At the same time you are provided with a new standalone/local client device installer (i.e. an executable) loading the new database version being installed on your server. The installer can be downloaded from the Installation Files section of the secure Thornberry customer Knowledgebase website at any time.

NOTE: Database version matching on server and standalone/local clients is not required from an InterSystems perspective, but is required from a practical perspective because the NDoc application is identical on both platforms and Thornberry developers may have chosen to implement features found only in the newer database. In the weeks leading up to your server upgrade you are advised as to the specific NDoc application upgrade for which standalone/local client upgrading is a prerequisite.

An approximate timeline is shown below:

- In July 2009, you are told about a Fall 2009 database upgrade from Caché ver. 2006.1 to ver. 2009.2.
- In July you receive server upgrade date options from Thornberry (date assignments are made on a first come, first served basis); you choose Nov 15, 2009.
- You learn from Thornberry that the December NDoc monthly update (9.12.01) will contain Caché 2009.2 features and cannot be installed on your server until standalone/local clients have their database upgraded.
- You have installed NDoc updates through October; your current NDoc version is 9.10.01.
- Thornberry performs your server's database upgrade on Nov 15; your NDoc version remains 9.10.01.
- You download and install NDoc version 9.11.01 on your server at your convenience.

- Thornberry posts and gives you access to a new 2009.2 standalone/local client installer.
- You upgrade your standalone/local client databases at your convenience by running the new installer on each standalone/local client.
- After all standalone/local clients are upgraded, you download and install NDoc version 9.12.01 on your server.

There are typically no updates to Caché other than these every 2-3 year database upgrades. However, in the rare event it becomes necessary for InterSystems to issue a critical fix, sometimes referred to as an "ad hoc" or "patch", to the database version deployed on your NDoc server and standalone/local clients, it will be applied by Thornberry to both on premise and hosted servers, and incorporated into a new version of the standalone/local client device installer posted to the secure Thornberry customer Knowledgebase website. You are notified by email of the new installer's availability on the website and of your responsibility to run the new installer on each of your standalone/local clients in order for the fix to be properly applied.

Updates to Caché require the standalone/local client to be brought into your agency in order for the new installer to be run by an IT professional. Caché upgrades are not performed by end users. Running the installer automatically upgrades the standalone/local client database to the new version, including any critical fixes. The upgrade deletes the old database, so the installer first uploads any patient charting to the server before starting the actual upgrade.

NDoc

Types of Updates

There are three types of updates Thornberry provides for NDoc: Major, Minor, Sub-minor. Each type has its own release cycle and definition of what is included.

Major

Major updates are generally referred to as "database upgrades". These updates typically only include infrastructure updates/modification, such as an upgrade to the HealthShare and Cache database platform that NDoc runs on. Major updates do not occur on a regular schedule but are on average once every 2-3 years.

Minor

Minor updates are generally referred to as "NDoc updates". These updates will include new features/interfaces and enhanced functionality. Minor updates are released more predictably, every 5-6 weeks.

Each minor update is fully described in accompanying release notes as well as a webinar you may attend in order to view the update's content demonstrated by a Thornberry clinician. Use the release notes and webinar to judge the update's impact on your agency and whether any staff orientation is required prior to installing the update.

Sub-Minor

Sub-minor updates are sometimes referred to as "patches". These updates will include critical bug fixes. Occasionally these updates may also contain experimental or beta features that must be manually enabled by Thornberry staff to have any effect. Sub-minor updates are released when necessary and created to repair defects in a minor update requiring an urgent fix.

Although minor updates are tested thoroughly before release, certain areas of NDoc are complex and difficult to test under every possible scenario. If a software "bug" is inadvertently released, the issue is evaluated for urgency. If the bug is not benign, its correction is designed, coded, tested and compiled into a

sub-minor update release. In a manner similar to the minor update itself, the patch is then applied to multiple Thornberry internal servers and tested again.

Versioning

NDoc's versioning system corresponds to the three types of updates. The format is: "{MajorVersion}.{MinorVersion}.{SubMinorVersion}", where each version is a two digit number starting at "01". When any version number increases, the latter versions in the format are reset to "01". The current NDoc version number can be found at the bottom right of the Home window.

Examples

- Major - 15.01.01, 16.01.01, 17.01.01
- Minor - 16.06.01, 16.07.01, 16.08.01
- Sub-Minor - 16.06.02, 16.06.03, 16.08.02

Managing Updates

NDoc Updates can be managed through the NDoc UI or by manually loading the update. When managing updates manually, you are responsible for installing all available minor and sub-minor updates available to get you to the desired update. From within the NDoc, updates can be manually scheduled or auto-scheduled based on update type. Multiple updates can be scheduled to install at the same time. Your NDoc System Manager will receive an email announcing when a new update is available.

Update Management via Manual Execution

Compressed ZIP files with instructions for manually loading an update are provided by Thornberry for agencies that don't wish to use NDoc's built in update system. The ZIP files can be downloaded from the Thornberry customer Knowledgebase portion of our website. The filename format is the version number without the separators (e.g. 17020100.zip, 17020300.zip). When running an executable update, that update is queued for installation, but if not run in a valid sequence, it will not actually be installed. In order for an update to fall within a valid sequence, it can only increment any version number by one. The latter version numbers are reset to "01" when a version number increases. Some examples of valid and invalid version sequences:

- Valid: 16.06.03 -> 16.07.01
- Valid: 16.07.01 -> 16.07.02
- Valid: 16.07.01 -> 16.08.01
- Invalid: 16.06.02 -> 16.08.01
- Invalid: 16.06.01 -> 16.06.03

Manually Running an Update

In order to manually run an update, you'll need to make sure you have access to Terminal with an account that has the %All role assigned to it.

1. Download the ZIP
2. Extract files
3. Open Manual_Install.txt and follow instructions under Installation

Update Management via NDoc

Updates can be managed in NDoc from the System Updates function. This function is only accessible to the System Administrator user type. The System Updates function provides users the ability to schedule updates to be installed at a specific time or configure automated update scheduling for sub-minor updates.

The System Updates function provides a list of updates that are available for installation. It also shows any currently scheduled updates and allows for the configuration of automated update installation.

NDoc automatically download the latest available updates. Every day at midnight, the NDoc server checks with the NDoc update server for any available updates. It will download any applicable updates and, if configured for automated install, setup a scheduled task to install the updates. Users can force a check at

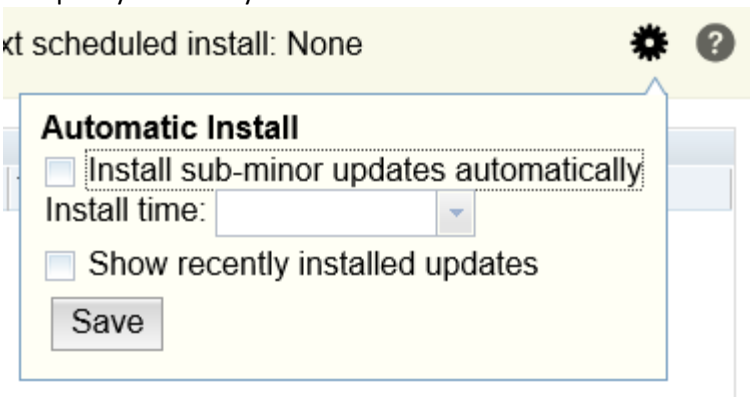
any time using the “Check for Updates” button in System Updates. **NOTE**: If NDoc indicates it is unable to reach the update server, please make sure the NDoc server can reach updates.thornberryltd.com.

You can easily find and review the Release Notes for any update by selecting the update you wish and clicking the “Release Notes” button. Installed updates are retained in System Updates for 14 days in order to easily find the release notes again.

Configuring Automatic Update Installation

1) In System Updates, click the Settings (“cog”) icon
2) Select to install sub-minor and specify the time you wish for installations to occur.

Automatic Install settings

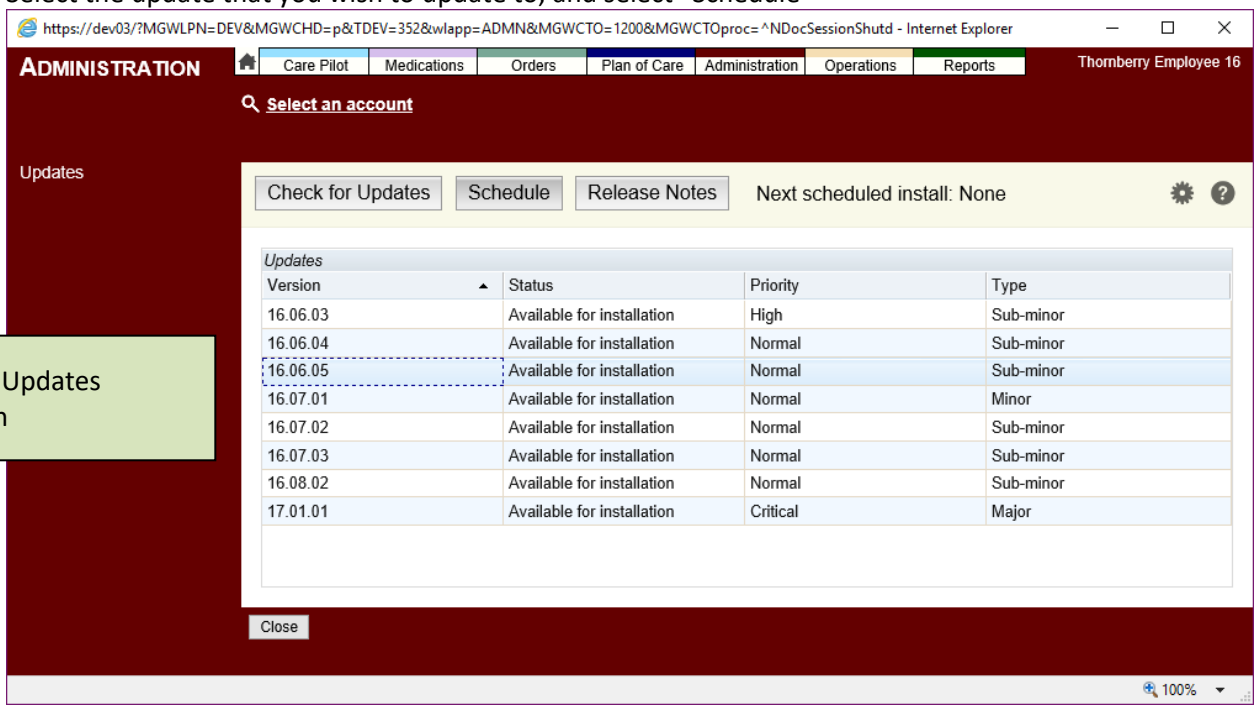


3) Click “Save”

Scheduling an Update for Installation

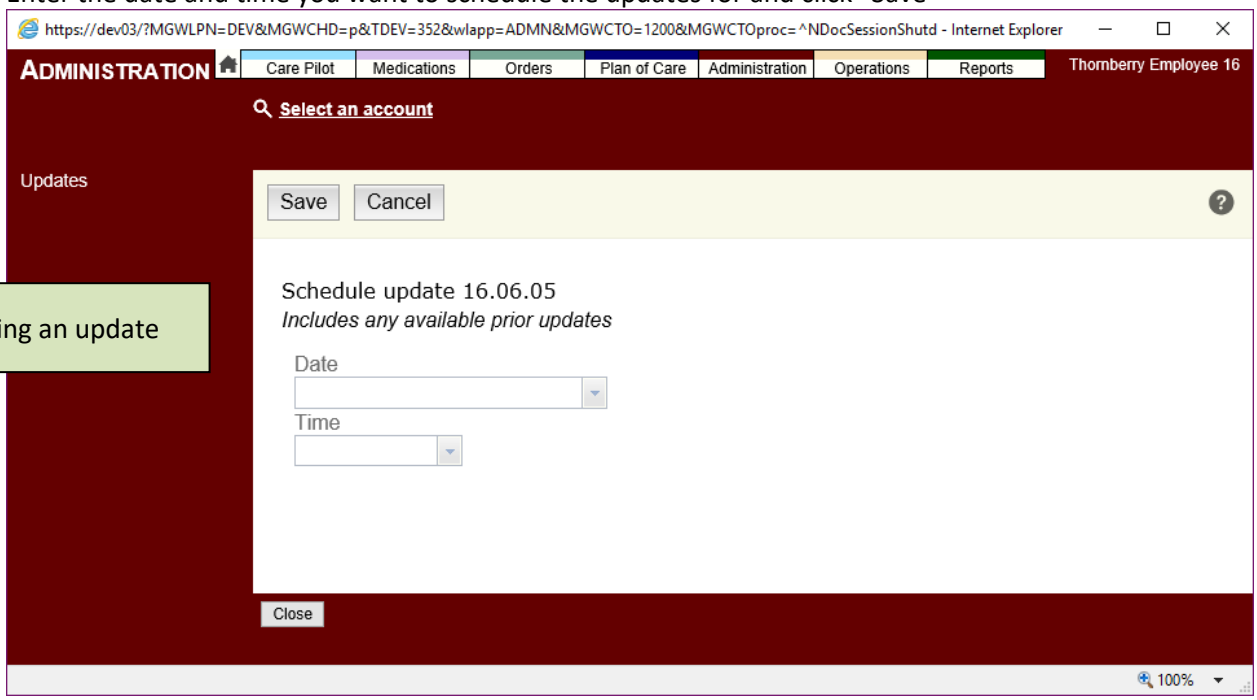
1) Navigate to System Updates
2) Select the update that you wish to update to, and select “Schedule”

System Updates function



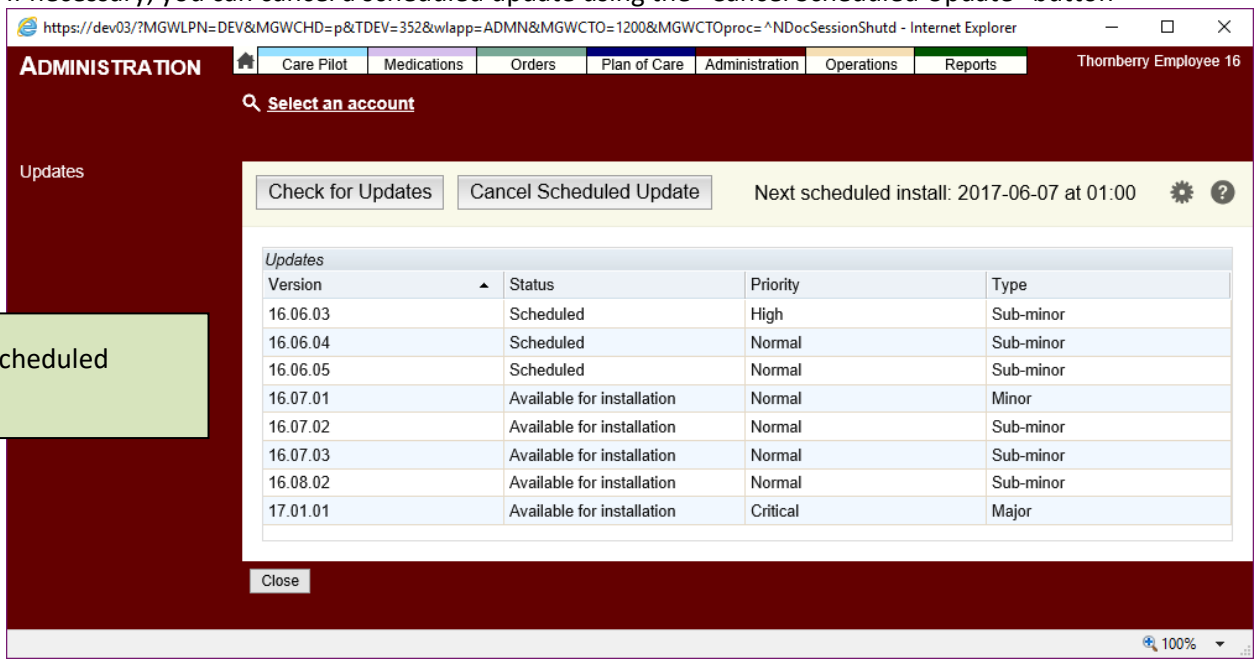
3) Enter the date and time you want to schedule the updates for and click “Save”

Scheduling an update



4) If necessary, you can cancel a scheduled update using the “Cancel Scheduled Update” button

Seeing scheduled updates

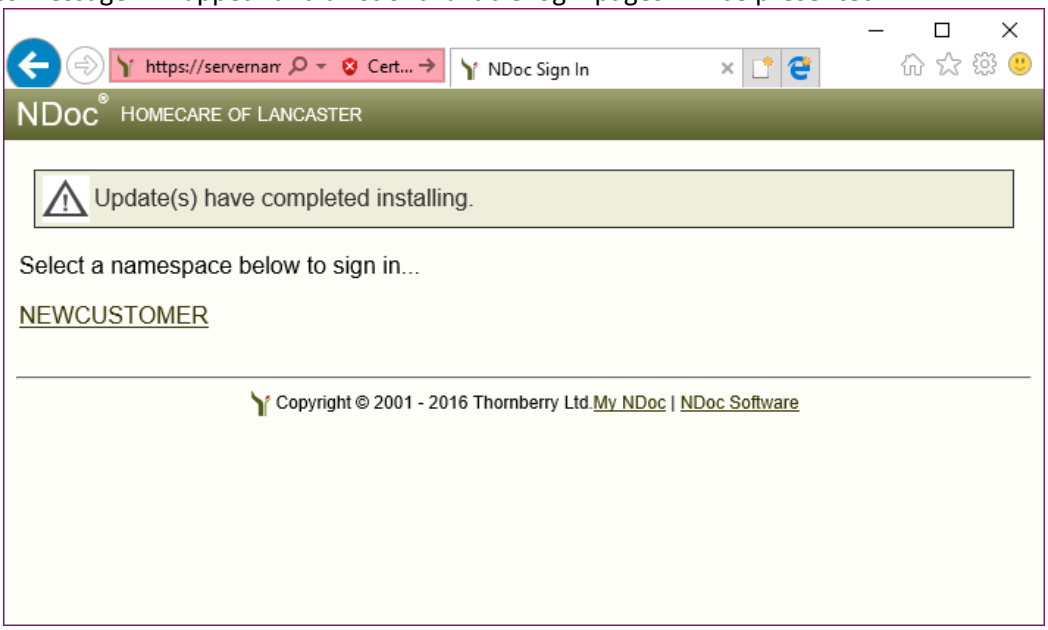


User Notifications

A notification will appear to any users that are logged into NDoc 5 minutes prior to the scheduled install time alerting them that an update is about to install and they should save their work. Once the update begins, any remaining users will be logged out of NDoc and redirected to an update install status page.

Monitoring Update Progress

Any users logged in while an update is running or anyone who navigates to the NDoc login page during an update installation will be redirected to the NDoc Update Progress page. Once the update is complete, a success message will appear and a list of available login pages will be presented.



NDoc Utilities

There are several NDoc utilities for securing the environment including setting password complexity, user ID creation, user types, system timeout, etc. These utilities help to prevent unauthorized access to NDoc and to make sure that only the proper employees have access to PHI.

Password Encryption

User passwords are encrypted using Password-Based Key Derivation Function 2 (PBKDF2) with HMAC-SHA; SHA-512. Since we use SSL for communications, during transport the password is encrypted and hashed for integrity. There is no NDoc reporting mechanism to see passwords, either internally or externally. A user must know their password or have it reset by the System Manager or Security Manager who provides a temporary password detailed in *Modifying/Resetting Passwords*.

Password Settings

When changed, they impact newly created/modified passwords from that point forward. There are default values for these settings, but they can be modified. NDoc password complexity could be set to match the settings of your agency's requirements. These apply at the server and standalone/local client levels (after a user syncs).

Accessing password settings

- Administration > System > Settings > Security

Enabling/disabling the setting

- A check enables the setting and causes the text fields to become active, removing the check disables it and the text fields gray out.

Modifying values

- We have provided default values, but they can be modified. 0 is not allowed for any field.
- Click in a field, type in a new value and either click on another field or Tab off it. Press Save to save the values or Cancel to discard your changes.

Password Length

The default is on, set to a value of 6. This determines the minimum length of the password.

Enforce Password History

The default is off. This is the number of times a user must use a new word when changing their password before being allowed to use an older password over again.

Maximum Password Age

The default is on, set to 90 days. This defines the number of days before a user must change their password. A user's 90 days begins again whenever the password changes.

Account Lockout Threshold

The default is off. This is the number of times a user account can be logged into incorrectly before it inactivates. The System Manager/Security Admin must then reactivate a user's account.

Automatically disable users who have not signed in for XX days

The default is off. This is the the number of days before a user's account is automatically disabled if they have not signed into NDoc. The System Manager/Security Admin must then reactivate the user's account.

Passwords Must Meet Complexity Requirements

The default is on with Uppercase (A-Z) and Base 10 digits (0-9). These complexity requirements force a user to use these types of characters in their password. A more complex password is more secure. Settings available:

- English uppercase characters (A-Z)
- English lowercase characters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric (ex: !, $, #, %, etc.)

Modifying/Resetting Passwords

Modification of a password occurs three ways:

- User changes their password on their own - After logging into NDoc, they go to Administration > Employee > Change Password where they enter their old password, then their new password meeting any password complexity requirements that have been setup. Standalone/local client users then need to sync afterwards to update their password stored on the server.
  The Maximum Password Age feature is on - The user receives a reminder from NDoc 10 days before the password is set to expire to change their password at which point the user would, as stated in the bullet above, change their password manually. On the day the password expires, the user is forced to change their password at login providing the old password and then their new password. Standalone/local client users then need to sync afterwards to update their password stored on the server.
  User forgets their password – When the user forgets their password, the process for resetting it depends on how the user is logged into the system.

Direct connection to NDoc

- User contacts Sys Mgr/Sec Admin
- Administration > Employee Table > Access > enter the Employee ID or User's name
- Create a temporary password and check the box for "User Must Change Password"
- Click Save.
- User logs into NDoc with the temporary password and creates a new password

Local connection to NDoc

- User contacts Sys Mgr/Sec Admin
- Administration > Employee Table > Access > enter the Employee ID or User's name
- Create a temporary password and check the box for "User Must Change Password"
- Click Save.
- The System Manager needs to sync the user's standalone/local client using the SYSMAN login to bring down the new password for the user's ID to the standalone/local client.
- User logs into NDoc with the temporary password and creates a new password. During their next sync, the new password gets sent back to the server

Assigning Equipment to Standalone/Local Client Users

For agencies using standalone/local clients, you need to assign an equipment ID to the user account before doing a refresh. This is important as NDoc uses the ID as a reference to the clinician to create patient data files assigned to that user during overnight processing. These data files, an aggregation of the patient's data from the previous day and historical charting are then transferred down to the user's standalone/local client when they do their first

synchronization of the day from the NDoc server. The process for doing this is detailed in the section *Creating or Changing the Standalone/Local Client Device ID*.

Client Device Settings

Agencies can control client security features through settings available under Administration > System > Settings > Security. These options are available within the Client Device Settings section:

Prohibit download of SSN, Medicare # and Insurance Policy #'s to clients? - Y/N

This setting is disabled for agencies by default. The activation is at the request of the customer at which time the scope and ramifications of this setting is explained further. This change will require a substantial review of internal workflow processes.

After synchronization: Do Nothing / Sign out on completion / Sign out on cancel:

This option gives agencies three methods to control what users experience after the client synchronization is completed. Specifically, these options operation as follows:

- **Do nothing** - Nothing will happen after the synchronization is complete. Your computer will stay on the synchronization screen, waiting for the automated synchronization.
- **Sign out on completion** - After your synchronization is completed, you will be signed out of NDoc, and will need to sign back in to continue working. This is the default value for the setting.
- **Sign out on cancel** - When you cancel out of the synchronization, you will be signed out of NDoc, and will need to sign back in to continue working. This is an automated process if this setting is configured.

Allow client to configure step 5: Y/N:

This option setting allows agencies to give users the ability to override the agency settings. In this case, users may want to change the setting to enable automated or multi-day syncs if the agency setting is set to prevent that option. However, for agencies who desire greater control over this process, the user override option may not be prudent.

Client Credential Details

The Security Settings page also includes credential details needed for the client install and refresh process explained later in the manual:

Client Caché Admin Account

This account can be used to log into the database on any client device synchronizing to this namespace.

Username:_____ Password: _____

Refresh/Synchronization Account

This account must be used to authenticate a client for a refresh and is used as part of the synchronization.

Caché Username: _____ Password: _____

Client Synchronization Resources

Success with ensuring patient data is updated correctly and clinicians are accessing the most up to date charting relies heavily on successful and disciplined client synchronization practices. The user resources to describe the client synchronization process is available via two documents as shown below via the secure Thornberry customer Knowledgebase website online resources.

- **FASTForm for Data Synchronizations**
- **Reference for Synchronizations**

Login Banner

The login banner allows the System Manager or Security Manager to create a customized banner letting non-agency users know it is illegal for them to access NDoc. It can be also be used for other information messages. The login banner can be modified in Administration > System > Settings > Login Banner. To modify the banner, follow these instructions:

- Enter the message that you would like to display (note: although most characters can be accepted within the textbox, users may wish to use Notepad or . It accepts all characters so you could create something in a text editor and copy/paste it here.
- When finished with inputting the text, you can click Save.

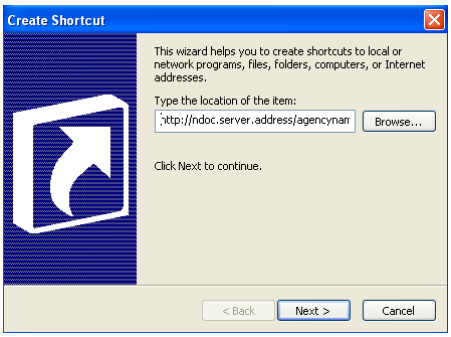
The banner displays immediately for those connecting directly to the NDoc server. For those on standalone/local clients, they do not see the new message until they synchronize their client.

Installation

Creating a Desktop Shortcut to Launch NDoc Start Page

To add a shortcut to the desktop that will open the NDoc start page in an Internet Explorer window:

1. Right-click on the desktop and select New→Shortcut
2. As shown below type your NDoc server's web address with the NDoc start page specified. The format is HTTPS://ndoc.server.address/agencynamestart.htm, where agency name (in the start page name) is the name of your agency as specified by Thornberry during the server's initial setup. Contact your Systems Administrator or Thornberry if you are unsure about the name associated with your start page.



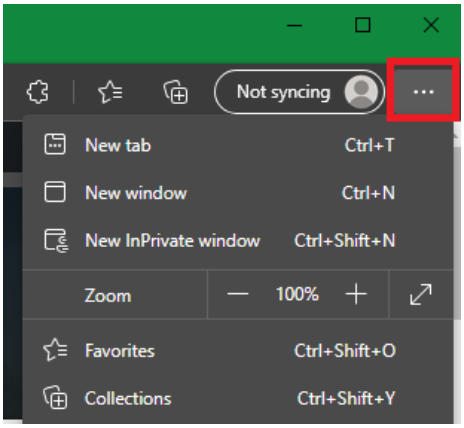
3. Click the Next button.
4. Click the Finish button.

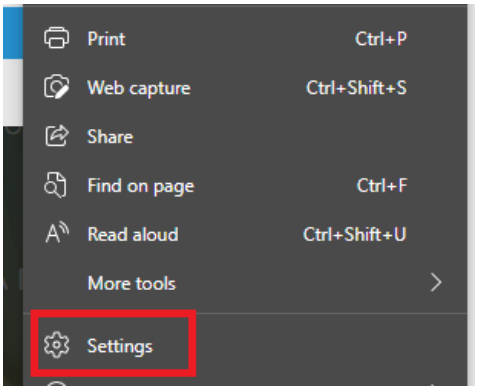
Microsoft Edge Browser Settings

Adding the NDoc Server to Microsoft Edge's Pop-Up Blocker exception list

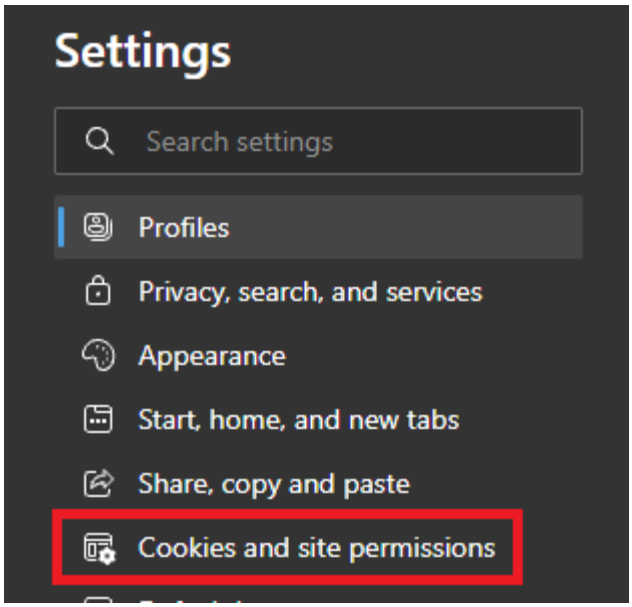
If your PC's Microsoft Edge settings include having the pop-up blocker turned on, you will need to add the NDoc server's web address (IP address or host name) to the list of allowable sites for the pop-up blocker. You can do this by taking the following steps:

1. In Edge, click the three dots in the upper-right corner of your window and Click Settings from the drop-down menu.

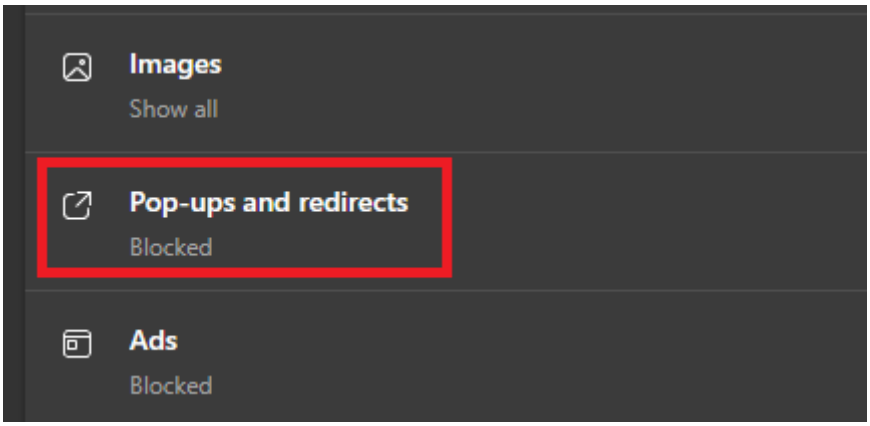




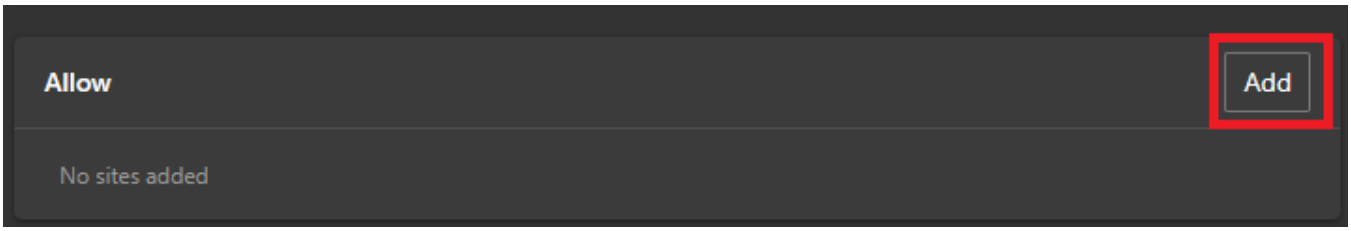
2. Under Settings, click Cookies and site permissions.



3. Under Cookies and site permissions, locate and click Pop-ups and redirects.



4. Click the Add button next to the "Allow" option. Then, enter your NDoc URL/web address and click Add to save the exception.

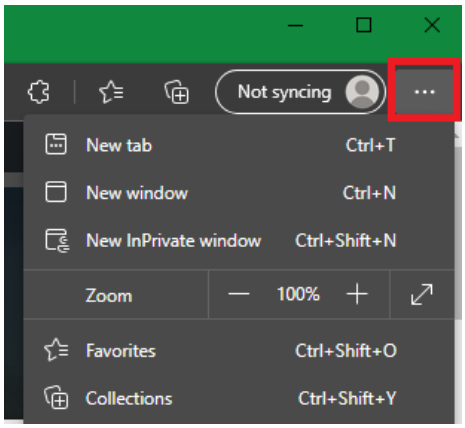


5. A failure to add your NDoc URL/web address properly to the exceptions will result in a message on the login page stating, "You must allow pop-ups from [your NDoc URL/web address] for this application to run properly.

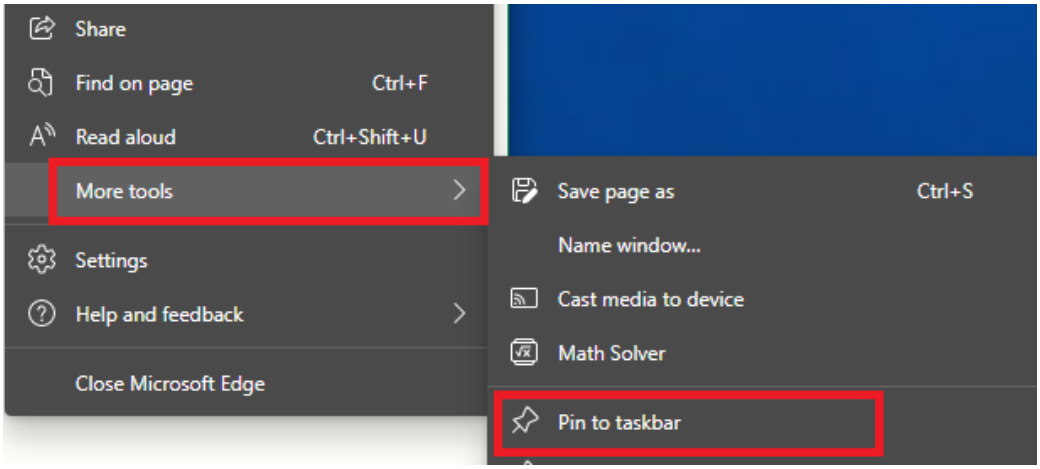
Creating a taskbar shortcut to launch the NDoc start page

The following steps create a taskbar shortcut that opens NDoc in Microsoft Edge within the Windows operating system.

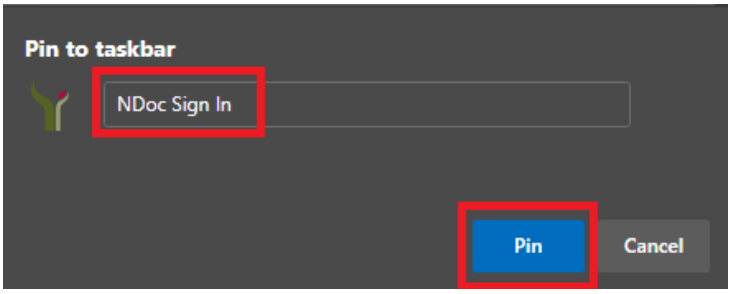
1. Open the Edge web browser.
2. Browse to your NDoc URL.
3. Next, click the three-dot icon in the top-right corner of the window.



4. Then hover your mouse over More tools and click Pin to taskbar.



5. Next, enter a name for your pinned website and click Pin.



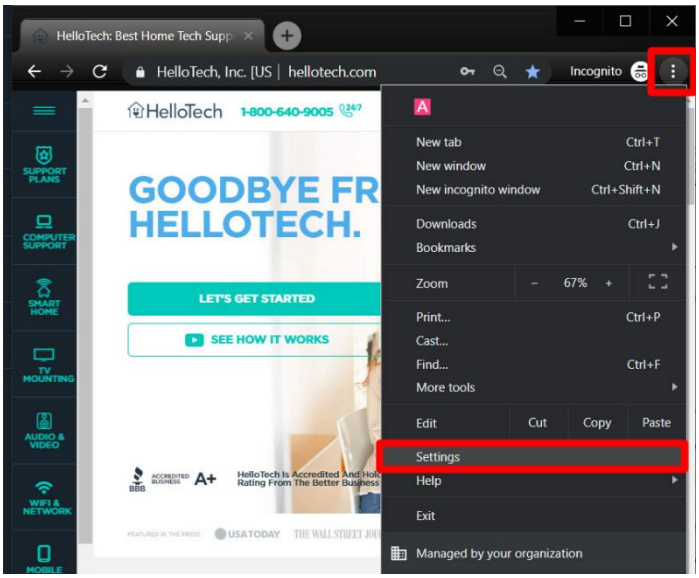
6. Finally, you will see your shortcut on the taskbar. This approach creates a taskbar shortcut with the icon of the website. Clicking this shortcut icon will open the website in the Edge browser.

Google Chrome Browser Settings

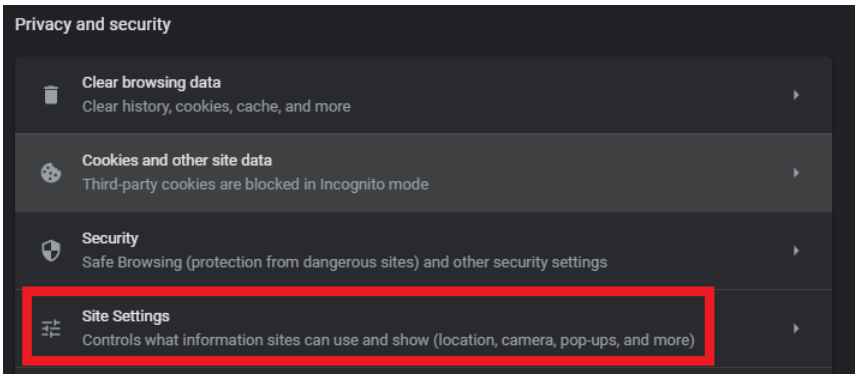
Adding the NDoc Server to Google Chrome's Pop-Up Blocker exception list

If your PC's or Android device's Google Chrome settings include having the pop-up blocker turned on, you will need to add the NDoc server's web address (IP address or host name) to the list of allowable sites for the pop-up blocker. You can do this by taking the following steps:

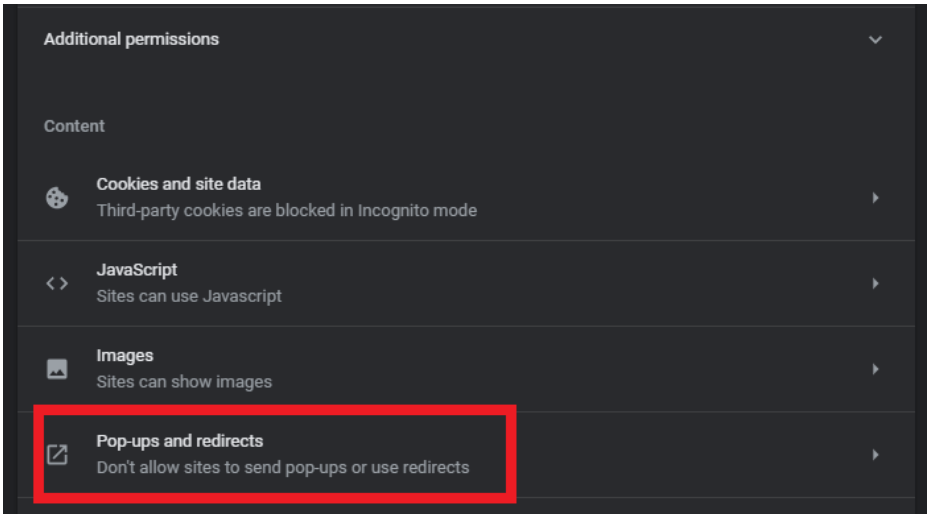
1. In Google Chrome, click the three dots in the upper-right corner of your window and Click Settings from the drop-down menu.



2. Under Privacy and Security, click Site Settings.



3. Under Site Settings, locate and click Pop-ups and redirects.



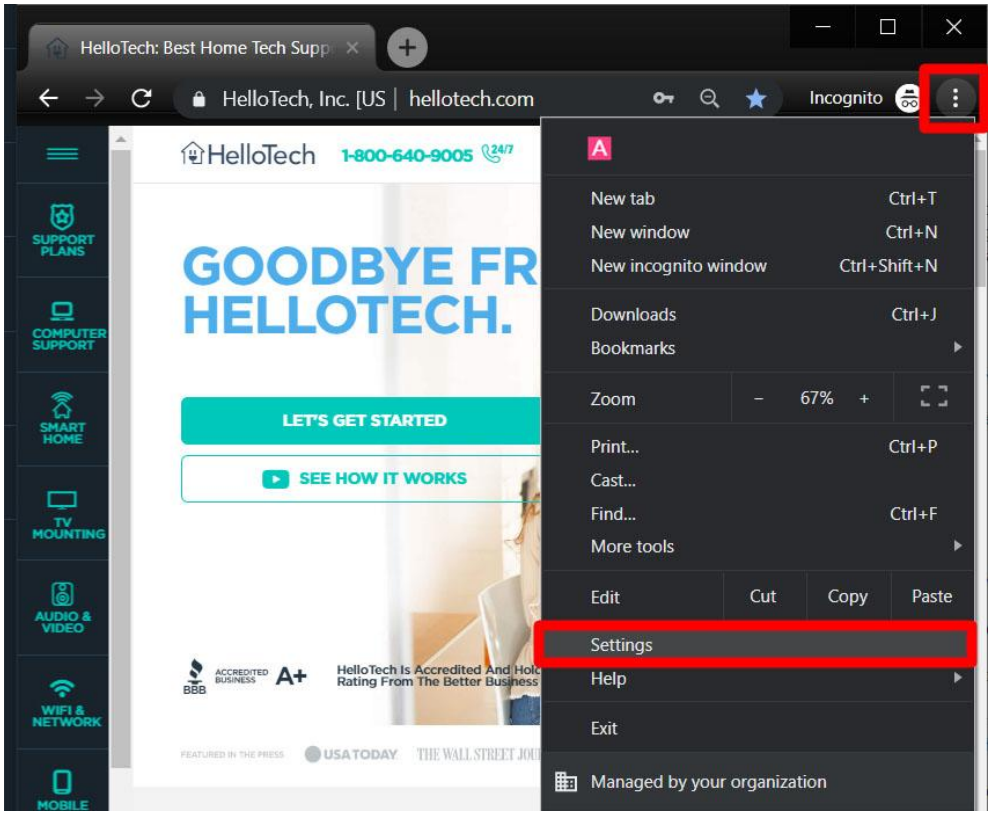
4. Click the Add button next to the "Allowed to send pop-ups and use redirects" option. Then, enter your NDoc URL/web address and click Add to save the exception.

5. A failure to add your NDoc URL/web address properly to the exceptions will result in a message on the login page stating, "You must allow pop-ups from [your NDoc URL/web address] for this application to run properly.

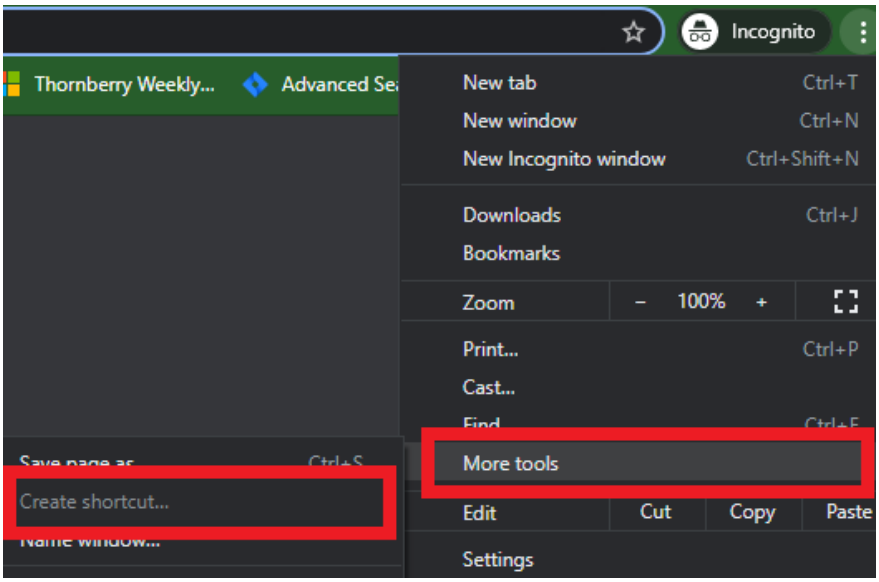
Creating a Desktop Shortcut to Launch the NDoc Start Page

The following steps create a desktop shortcut that opens NDoc in Google Chrome within the Windows operating system. Open the Chrome web browser.

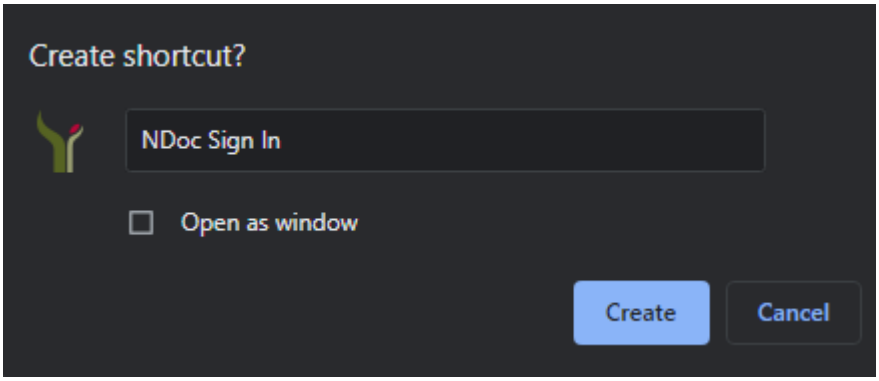
1. Open the Chrome web browser.
2. Browse to your NDoc URL.
3. Click the three dots in the top right corner of the window.



4. Hover your mouse over More tools and click Create shortcut.



5. Enter a name for your shortcut and click Create. You can also check the Open as window box to have the website open in its own browser window. If you do not check this box, NDoc will open in a new tab of your existing browser window.



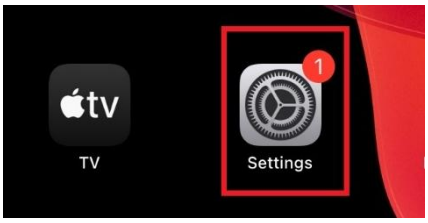
6. Finally, you will see your shortcut on the desktop. This approach creates a desktop shortcut with the icon of the website. Double-clicking this shortcut icon will open the website in the Chrome browser.
7. Once you have created a desktop shortcut on a Windows 10 computer, it can also be found under your Recently Added apps and in the Chrome Apps folder in your Start menu. You can then right-click the icon to add it to your Taskbar or your Start menu.

Safari Browser Settings

Turning off the Pop-Up Blocker in Safari on an iPad

The iPad iOS only allows for the Safari Pop-Up Blocker to be enabled or disabled for all sites. Customers who wish to use NDoc on an iPad would be required to turn off the pop-up blocker while using NDoc via the steps below.

1. Open Settings on the iPad by clicking the Settings gear icon.



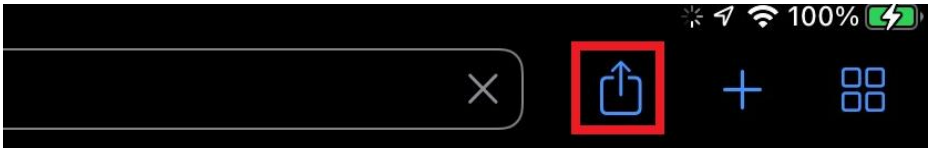
2. Scroll to the Safari icon and click it.

3. Scroll to the setting, “Block Pop-ups” and slide the button to the off position.

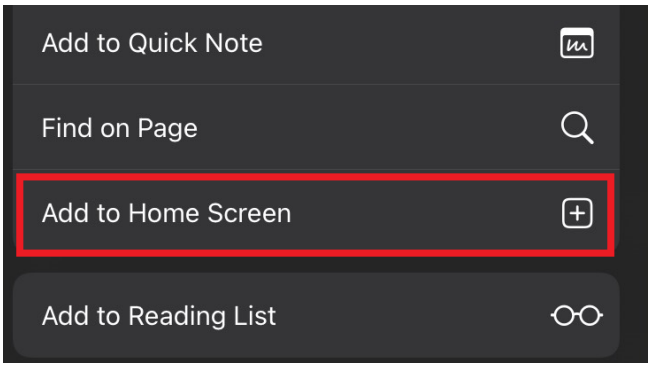
Creating a Home Screen icon to Launch the NDoc Start Page

The following steps create a Home Screen icon that opens NDoc in Safari on the iPad iOS.

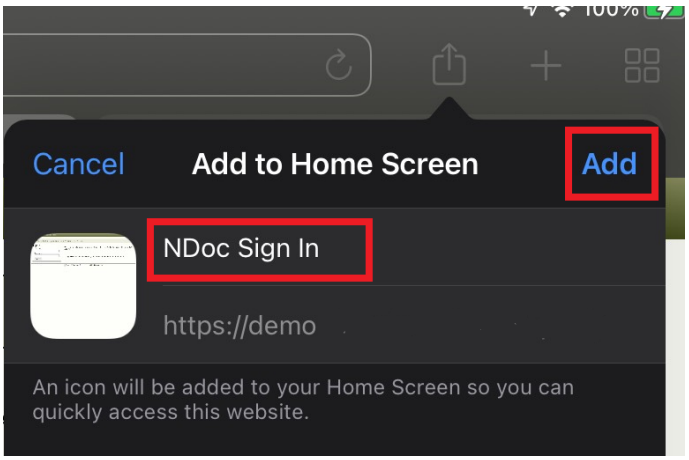
1. Browse to your NDoc URL in Safari.
2. Tap the "Share" icon.



3. Scroll down and tap "Add to Home Screen."



4. Tap the shortcut name to edit to your preferred text, then tap "Add" to close the window and display the icon on the Home Screen.



NDoc Standalone (Local) Client Installation

This section guides you through the installation of the NDoc software, which utilizes the Caché database software as a back-end on all client installations. These instructions guide you through the process of preparing and executing the *NDocClient* file to install NDoc, performing manual configuration steps for Caché and NDoc (if necessary), and synchronizing the client for the first time.

Instructions for performing specific install scenarios, such as silent and/or logged installations, and steps for troubleshooting can be found later in this section. It is recommended you review the section in its entirety before beginning any part of the installation as there are many options available to implement based on your agency's requirements.

Preparation

If this is your first time installing NDoc on a client machine you should review each of the following sections in preparation for performing the installation. Below is a *Checklist* for those familiar with the process. If you have issues installing please refer to the *Troubleshooting* section.

Checklist

1. The user receiving this installation on their device must have assigned to their User ID a 4 digit Device ID in NDoc on the server. See *Creating or Changing the Standalone/Local Client Device ID* section for more details.
2. Microsoft .Net Framework 4.6.1 installed
3. Java JRE version 8 update 222+ (Oracle® or OpenJDK) installed
4. Required Files:
   - NDocClient_v.X.xx – Available from the secure Thornberry customer Knowledgebase website under Installation Files.
   - Cache.key – Refer to the File Download FASTForm for details on how to download the key file.
5. Optional Files:
   - Standalone/local client refresh files – for areas with slow connection speeds, going to the location mentioned above for the Cache Key, under NDoc Restore Files, 3 files can be saved locally to make a refresh faster: lib.7z, lib_fdb.7z, and Tables.7z. Refer to the File Download FASTForm for more details.
   - connect.vbs and unconect.vbs; connectBroad.vbs and unconectBroad.vbs

     Note: Reference the *Automating Connections for Synchronization* document of this manual and the *Features List* section of this document for more information.
6. Review the *Features List* section for required and optional features for your installation and necessary pre/post configuration steps (depending on install type).
7. Follow the instructions based on the type of install you will be performing, either Installing the NDoc client manually or Installing the NDoc client via automated scripted execution
8. Perform synchronization connectivity test(s).
9. Perform any post-configuration steps, depending on features selection. See the *Features List* section for details.

Installing as Administrator

Running the NDoc setup executable on any Windows OS requires User Account Control elevation by running the installation as an administrator. If you do not currently have administrative access to the machine, you can right-click on the executable file and select "Run as administrator" to start the installation. If you are performing any command line based install this can be done by commands in a DOS prompt again running as the administrator.

Creating or Changing the Standalone/Local Client Device ID

There are two main steps to create or change the standalone/local client device ID. The ID must be setup on the server and then assigned to the client. This ID is what prompts NDoc on the server to create user assigned patient files for download to the user's device. You can keep track of your standalone/local client IDs by going to Administration>Employee>Assign Client Devices>Print Client Assignments. The initial NDoc server installation will include an initial inventory of client ID's (1001 through the number your agency has purchased; i.e., if 25 standalone/local client licenses were purchased, NDoc will be initially installed with an inventory of 1001 through 1025).

ID Configuration on NDoc Server

1. Create the 4-digit device ID on the NDoc server.

   Note: Client IDs cannot include a leading zero. **The Client ID cannot be "9999".**

   NDoc by default includes a number of client IDs as 'unassigned', corresponding to your initial license quantity. If this is a new client, subsequent to your initial quantity, you must create an entry for it, status 'unassigned', for it to successfully sync. You should skip this step otherwise.

   Log into NDoc on the server as a user with the System Manager user type (default: SYSMAN). Go to Administration>Employee and the Assign Client Devices function. Select the Add option at the top of the page. Enter the client id in the *Local Client ID* box. **NOTE:** If your goal is to simply test your client installation, you may leave the option *Status* as 'Unassigned', click Save on the bottom menu, and skip the step 2. In the *Synchronization Connectivity Test* section, use your SYSMAN login on the client to synchronize it to the server.

2. Assigning a user to the client on the NDoc server (optional)

   You now establish the link between this client and the clinician's user ID who will use the client on a regular basis. Select the Change option at the top of the page and then select the client you would like to assign from the list of client IDs. With the client ID selected, you should now select the user id you would like to assign to this client from the box below. Click Save to finish.

ID Configuration on Standalone/Local NDoc Client

Assigning the 4 digit ID when installing the NDoc client

Setting up the client's initial 4-digit ID is done when refreshing the client after the install of NDoc.

Modifying the 4 digit ID on the client

To modify a client 4 digit ID, for example due to an employee change or perhaps a swap out of technology, you refresh the client. If it has been in use and has charting on it from the clinician currently using it, the refresh syncs the previous clinician charting (their visits) to the NDoc server.

Obtaining NDoc Client Installation File

Setup first requires you downloading the latest NDoc installer executable. The latest version can be downloaded from the Thornberry customer Knowledgebase website by logging in with your credentials. Contact your System Manager if unsure of your login information for client access.

Downloading the Cache.key (and optional Refresh Files)

Before executing the NDoc Setup installation wizard, you must download a license key for the Caché database software that is required by the install wizard. The file can be downloaded through NDoc or via *File Transfer [SFTP]*. The file transfer method is described below and is dependent on whether your site implements SFTP for client-to-server synchronizations. Refer to the File Download FASTForm for more details on how to retrieve this file through NDoc on the server as well as the optional client refresh files.

File Transfer

Using your preferred SFTP client login point the SFTP address to your NDoc server's IP or hostname address. Use the username and password for SFTP provided by Thornberry Ltd.

From the `<ftproot>\`*`YourAgencyName`*`\` directory, download the **Cache.key** file.

Place this file somewhere you can browse to on the client to which you are installing NDoc.

Connection Script Files (Optional)

Depending on your synchronization connection requirements you may want to setup connection script files before or after the install that can automate connection to a phonebook connection (e.g. VPN). For more information on the creation, configuration, and operation of connection script files reference the *Automating Connections for Local Client* Synchronization section.

Features List

The NDoc installer comes with many different features that can alter the installation in a pre specified manner. Some of these features are required for the installation to succeed, while others may be left off without affecting the success of the installation. The features are separated into two tables below, required and optional. The information is presented in three columns: the feature as it appears in the GUI (*possibly the window name*), the setting as it will be referenced when used in a scripted install, and a brief description/summary of what the feature will implement when used. It is highly recommended to review the details of all of the features described in further detail following the tables in this section.

Certain NDoc features denoted by ** are optional for install, but must still be implemented through some pre or post configuration process in order for NDoc to function properly. Details of what must be implemented for each feature are in its corresponding section following the tables below.

The table below lists a **required** feature and the next table lists **optional** features:

Feature (in GUI)	Setting	Description
Cache key import	**CKEY_DIR**=<FullPathtoFile>	Path to the cache.key file, surrounded by quotes.
Cache Administrative Password	**PW**=<Admin Password>	The administrative password for the Cache install surrounded by quotes. If this parameter is not included, the installer will quit out without completing the install.

Optional		
Feature (in GUI)	Setting	Description
Override Automatic Sync Time	SYNC_TIME_SECONDS=<*Time*>	Time of the day to start the automated synchronization (in seconds)
Power Settings Configuration**	**POWER**=<TRUE|FALSE>	Creates/Configures an NDoc power scheme based on current power scheme [Default: FALSE]
Shortcut Selection	**SHORTCUT**=<*Options*>	Allows you to define where you'd like shortcuts to be created. *Options* is a semicolon (;) delimited list of any combination of: STARTMENU — Creates shortcut in start menu TASKBAR — Pins the item to the taskbar DESKTOP — Creates shortcut on desktop
Shutdown Script**	**SHUTDOWNSCRIPT** = *<TRUE|FALSE>*	Shutdown script that makes sure that Cache shuts down properly on normal system operation
Logged Installation**	**LOGGED**=*<TRUE>*	Together with LOGFILE, logs output of the installer to a new file, in an existing directory [Default: FALSE]

	LOGFILE=<Full Path and File Name>	When LOGGED is true, this will create the specified file with logging information. The directory must exist already. Path should be surrounded by quotes.
Uninstall**	UNISTALL=<*TRUE*>	Allow the uninstall of current client version, along with older versions [Default: FALSE]
Java Configuration	**JAVA=**<Full Path to JRE>	Path to the Java JRE, surrounded by quotes.

** Optional for install, but must still be implemented through some pre or post configuration process in order for NDoc to function properly.

Power Settings

Depending on the use of NDoc there are some modifications, listed below, **that must be made** to the Windows power management settings. Even if the option to modify the power settings is selected, there are still some modifications that may need to be made for NDoc to perform properly based on your day-to-day usage. All the items listed below describe use cases of NDoc, where it is necessary for the modification to the power settings be made.

Hibernation**	Disable	Hibernation must remain off while NDoc is in use. Turning on hibernation may interfere with the client's ability to perform an automatic synchronization.
Monitor Timeout**	On Battery = 3 min Plugged In = 3 min	These settings do not affect NDoc and may be changed as necessary.
Disk**	On Battery = Never Plugged In = Never	The disks must remain running while NDoc is in use. Adjust this in relation to your NDoc timeout settings.
Standby**	On Battery = Never Plugged In = Never	Standby must remain off while NDoc is in use. Turning on Standby may interfere with the client's ability to perform an automatic synchronization.
Auto-Reboot after Windows update install	Disable	This setting can cause the client to reboot while waiting to complete an automatic sync. Disable this to prevent issues.
Laptop lid closure	On Battery = Do nothing Plugged In = Do nothing	Disable this setting to prevent issues to enable the ability to stay logged into NDoc with the lid of the laptop closed.

** Implemented by the NDoc setup installation when the power settings feature is enabled.

Firewall Rules

For NDoc to communicate properly on the network, certain firewall rules must be added to the Windows firewall or any other firewall solution in place. Below is a list of the firewall rules that are added to the Windows firewall when the installation is executed.

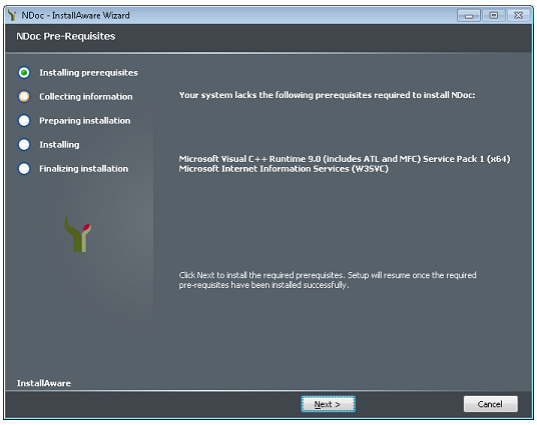
Ctelnetd.exe	Inbound – TCP [Telnet]
Sync	In/Outbound – Port: 7002 – TCP

winscp418.exe	In/Outbound – TCP [SFTP]

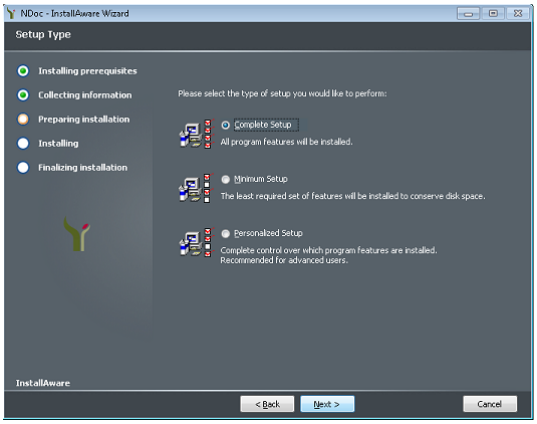
Installing NDoc client file

Run the executable and make sure you have administrative privileges by or right-clicking and select Run as Administrator. The expected overall install process takes an estimated 30-45 minutes, due to amount of tasks being performed; including installing Caché, installing and configuring IIS, etc. Runtime varies depending on PC hardware.

When you first run the executable it will take a few minutes to unpack all of the files to a temporary directory, during which you will see a progress bar. Once this is completed, the installation will check your system for the minimum requirements of NDoc and also validates if your system is missing any prerequisites that are needed for NDoc to install. If you are missing any of the necessary prerequisites, the installer will alert you with a list of the prerequisites that are missing in a window.



When prompted with the list of prerequisites to install, click Next to proceed with their installation. You will be prompted for basic installation setup information through the next few prompts, until you reach the setup type screen (image 4.2). At the setup type screen, you must select the type of install you would like to perform. A **Complete Setup** will install all of the features mentioned in the *Features List* section of this document, while a **Minimum Setup** will install only the necessary components of NDoc and none of the items in the *Features List* section. The **Personalized Setup** will allow you to select which features you want to install from the list of optional features shown.

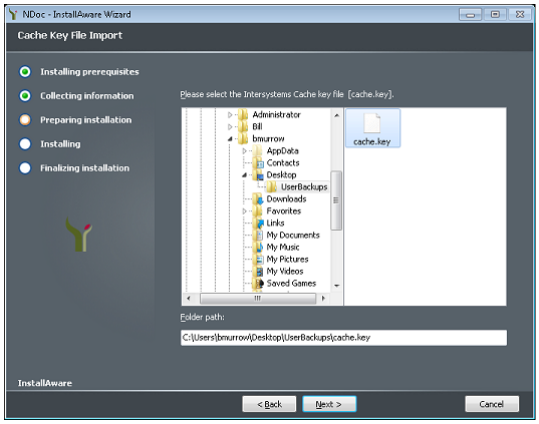


Features that will not be installed are marked with a red X in the feature select button. If you choose to perform a **Minimum** or **Personalized Setup** you should review the *Features List* section of this document for further instructions on setting up the computer for NDoc, since some optional features must still be configured in order for NDoc to function properly.

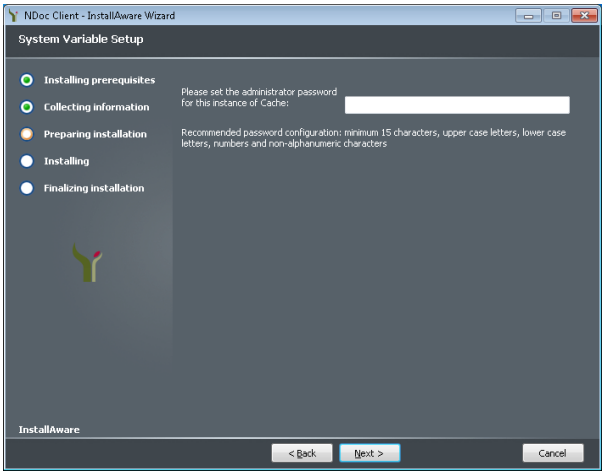
Now that you've selected the setup type and optionally toggled any features on/off, you should click **Next** to proceed. The next screen is the shortcut selection screen (image 4.4). Here you may select where you would like NDoc to create shortcuts. Once you're finished select **Next** to proceed.

At the following window you may optionally change the time at which NDoc performs an automatic synchronization. To do so, pick the hour, minute, and am/pm selection from the drop-down lists that apply to the time you would like to change this to. Click **Next** to proceed.

The next screen will prompt for the cache.key file. Navigate to the file and click **Next** to proceed at each of these screens.

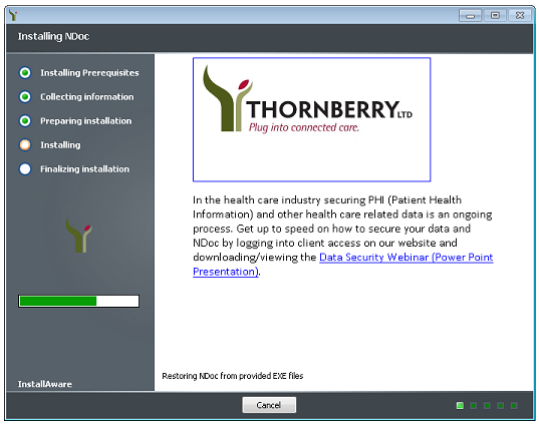


After providing the cache.key file, you will come to a screen prompting you for an administrative password for Cache. Although it's not expected for users or IT administrators to use this password during normal execution of NDoc, this password should be unique to each instance of Cache to limit the scope of damages should one of the passwords become compromised. Click **Next** to proceed.



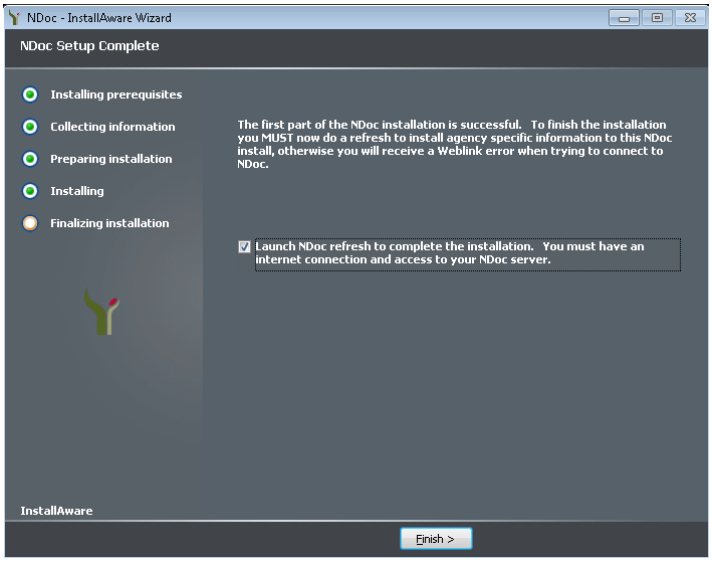
After providing the administrative password, you will come to a screen prompting you to choose the name of the Start Menu group that will be designated for the NDoc application. Click **Next** to proceed.

At the following screen, click **Next** to begin the installation. While the installation runs you will see a progress bar and status.



Once the installation finishes, you are informed the first part of the installation is done and that you can now refresh the device. Before refreshing, you need to have a Client Device ID created on the NDoc server to assign to the device. Creating the client device ID is detailed in the section *Creating or Changing the Standalone/Local Client Device ID*.

Keeping the option checked shown below launches your default browser window to the NDoc refresh page detailed in the section Refreshing a Standalone/Local Client. If you choose to refresh at a later time, the created shortcut on the desktop takes you to the refresh page. You are not able to access the login page until the refresh is finished. If you have an issue with refreshing please refer to the *Troubleshooting a Standalone/Local Client Refresh* section.



Automating NDoc client install via scripted execution

This section provides some examples of scripted NDoc client installations with options like silent and logged. You should refer to the section *Features List* for details on how to implement each feature in a scripted install.

Command Line

NDoc setup supports command line parameters for silent and logged installs. In addition, you may also set/override the values of variables used in your installation from the DOS command line.

Example – Silent install:

> NDocClient_vx.y.exe /s PW="server password" CKEY_DIR="c:\NDocInstall\"

Example – Setting required and select optional NDoc features:

> NDocClient_vx.y.exe /s PW="server password" CKEY_DIR="c:\NDocInstall\" JAVA="c:\Program Files\Java\jre1.8.0_144"

Example – Setting features with silent install:
> NDocClient_vx.y.exe /s PW="server password" CKEY_DIR="c:\NDocInstall\" IE=TRUE SHORTCUT=STARTMENU;DESKTOP

Example – Creating log file:
> NDocClient_vx.y.exe /s PW="server password" CKEY_DIR="c:\NDocInstall\" LOGGED=TRUE LOGFILE="C:\NDocInstall\setup.log"

Example - Silent Uninstall:
> NDocClient_vx.y.exe /s PW="" REMOVE=TRUE

Java

NDoc supports Java Runtime Environments (version 8) from Oracle and OpenJDK for the required functionality needed for both the application server and the offline clients. It is the customer's responsibility to maintain current versions of the Java Runtime Environment on both the server and offline clients.

OpenJDK Java Runtime Environment (JRE)

Availability

The OpenJDK JRE is available in a Windows binary at https://adoptopenjdk.net/. NDoc is supported by version 8 of the JRE (not any other version). On the site's main page, you will see the latest download version, based on whether you are running a 32 bit or a 64 bit workstation when connecting to the site. You will want to choose the version (OpenJDK 8[LTS]) and the Java Virtual Machine (HotSpot), and then the download button will populate the newest version of the Java Development Kit (JDK) (with JRE). The current version, as of this notice is version 8, update 222.

Installation

Graphical

Once you have downloaded the latest release, double click on the MSI file to start the installation. Read and accept the license if you are happy with the terms. On the Custom Setup screen you can choose the features that you want to install and optionally change the default installation directory. By default, AdoptOpenJDK installs to c:\Program Files\AdoptOpenJDK\<package> with the following features, which you can deselect, if necessary:

- Add the installation to the PATH environment variable
- Associate .jar files with Java applications

Additional features can be selected by clicking on the directory tree where you see a check mark (x). These features include:

- Updating the JAVA_HOME environment variable (this step is necessary for Cache / NDoc to recognize the installation of the JRE)

When you have chosen all the features that you need to install, click Next, then click Install to begin the installation. When the installation is finished, click Finish to close the installer. If Cache is already installed on the machine, you will need to right click on the Cache cube, and restart the Cache instance. This will force Cache to pick up the changes to the JAVA_HOME variable in Windows.

Command line

The OpenJDK MSI file includes the options to run the install silently on the command line. For the full list of options and examples, please refer to the Installation page on the AdoptOpenJDK site.

Upgrading from Oracle Java JRE

Before proceeding with the upgrade from Oracle Java to OpenJDK, you will want to have your IT team do an evaluation of all software on the machine that is using Java, and confirm that OpenJDK will work for all software involved. After receiving that confirmation, you will need to uninstall the Oracle Java software from the Add/Remove Programs area, before installing the OpenJDk software, following the instructions above or from the OpenJDK website.

Synchronization Connectivity Test

After completing the initial refresh it is recommended to test the synchronization process. For the most accurate simulation of a standalone/local client in the field, you should log into both Windows and NDoc using the credentials of the employee to whom the client will be assigned.

Run a LAN-based sync first, then test a dial-up, then broadband if desired (these options are toggled by the radio button in the synchronizations' **Step 1**). For **Step 2**, select Synchronization, and then click Start.

For troubleshooting, please refer first to the client c:\comm\log\comm.log file which could point to where the failure is occurring and refer to the troubleshooting section below for help on understanding common synchronization issues and error messages.

The amount of synchronizations allowed by a unique user ID is limited by the client license of the contract. Using the SYSMAN (System Manager) account is useful for this process, because the normal restriction for the account to be assigned to the device and the aforementioned limit is not enforced when using the SYSMAN account to synchronize. If the limit is reached you receive a message stating so. This does not reset until after Nightly Processing.

Note: You are not required to complete both a dialup and broadband sync, but it is highly recommended that you test all options that will be accessed by the user.

Troubleshooting

This section contains some basic errors that might occur during installation with some troubleshooting steps. When reporting these issues to the Thornberry Help Center sending us the text or screen capture of the error messages is always helpful.

Installation

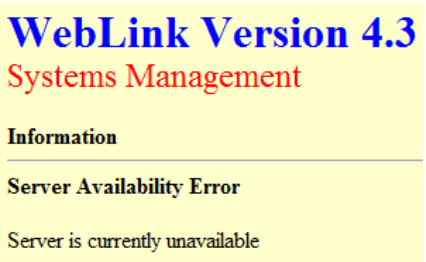
Problem: Invalid Application error appears after installation completes and the refresh page launched. The message continues to appear on all subsequent attempts to go to the login page for NDoc.

Solution: Delete all browser history and refresh the page

Startup and Synchronization

This section contains several error messages for NDoc not starting or syncing, followed by some possible solutions to the issue. **Note:** %WINDIR% refers to the Windows installation directory.

Server Availability Error. Server is currently unavailable.



Make sure the C:\NDoc\Intersystems\mgr\cache.key is a valid file and is the cache.key supplied by Thornberry for local client use. Another possible reason is due to the Caché database not being started. Look in the System Tray for the Caché cube and if gray, right-click and choose Start Caché. If Caché continues to not start, then it might be corrupted. Refer to the *Clearing out Caché journal information* section to fix it.

A webpage does not display

Make sure that http://127.0.0.1 is in the trusted sites and the Temporary Internet Cache is cleared. Also the ASP.NET might not be properly registered with IIS. Follow these steps below:

1. Click Start and in the Programs Box, type CMD. It should display in Programs. Right click on it and choose Run as Administrator. This opens a DOS Window.
2. Change directory as follows:
   For 32-bit machines change to: cd %WINDIR%\Microsoft.NET\Framework\v4.0.30319\
   For 64-bit machines change to: cd %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\
3. Run the command 'aspnet_regiis.exe -i' and press enter.
4. Close the DOS Window, reboot the PC and go to the webpage again.

Dial-up synchronization will not work

1. Make sure you have set up a dial-up networking entry. NDoc client synchronizations use %WINDIR%\connect.vbs to call the default dial-up networking entry and %WINDIR%\unconect.vbs to disconnect the dial-up session. Note: %WINDIR% refers to the Windows installation directory.
2. Navigate to and double-click on %WINDIR%\connect.vbs. This should invoke the default dial-up networking connection. If it doesn't:
    a. Locate the dial-up networking entry in Network and Dial-up Connections.
    b. Force a connect (right-click, then left-click on Connect).
    c. Enter the username and password (the Windows login) of the clinician that will be using this client and click Save. Make sure the username is valid and will authenticate on your network once the connection is established.
    d. Click Dial to start the dial-up sequence, then click Cancel.
    e. Repeat the forced connect to ensure the username/password have been saved; click Cancel.
    f. Return to %WINDIR%\connect.vbs; double-click; the dial-up networking entry should be invoked. Once you have verified that connect.vbs brings up the dial-up networking entry, you can be certain NDoc dial-up synchronization will work.

Automatic synchronization fails to start automatically

This is most commonly caused by the Caché Controller for NDoc service having insufficient access to start background tasks. See the *Caché Controller Service Configuration* document under the *Supplemental Procedure* section of this manual for information on setting the service up with administrative access to perform background tasks.

Synchronization starts but does not complete without error

1. Check permissions on the server's comm directory. The Default SFTP Site sync user (probably PROG) must have full control of this directory.
2. Check if the user id you are using is valid on the server.
3. If you performed your database upgrade with the September update installed (i.e. no later updates), then you should use the 'Reset Lastfile.txt' option in the System Manager Dashboard of the Administration module.

Refreshing a Standalone/Local Client

Follow the steps outline in 'To refresh a client' below for a fresh install of the NDoc client to a PC or as a means to correct other issues with NDoc.

A "refresh" consists of downloading partial backups, created daily, to the local client and restoring it to the database, along with applying any specific configuration changes.

To speed up the process of the refresh due to a slow LAN or internet connection, you can download 3 files from the server to the client. These files can be found via Administration > System > Downloads > Client Installation. If you have access to the server's file system, you can also find the files in the directory listed in Administration > System > Settings > System (Client Devices > Backups Path). The three files you would copy are Tables.7z, lib_fdb.7z and lib.7z. These files are updated daily, so any day you do a refresh you need to download the new files. The files then need to be placed in a folder on the client in C:\NDoc\Restore\ which you need to manually create. Refer to the FASTForm for the File Download function for further details if needed.

Refreshes Unrelated to Installation

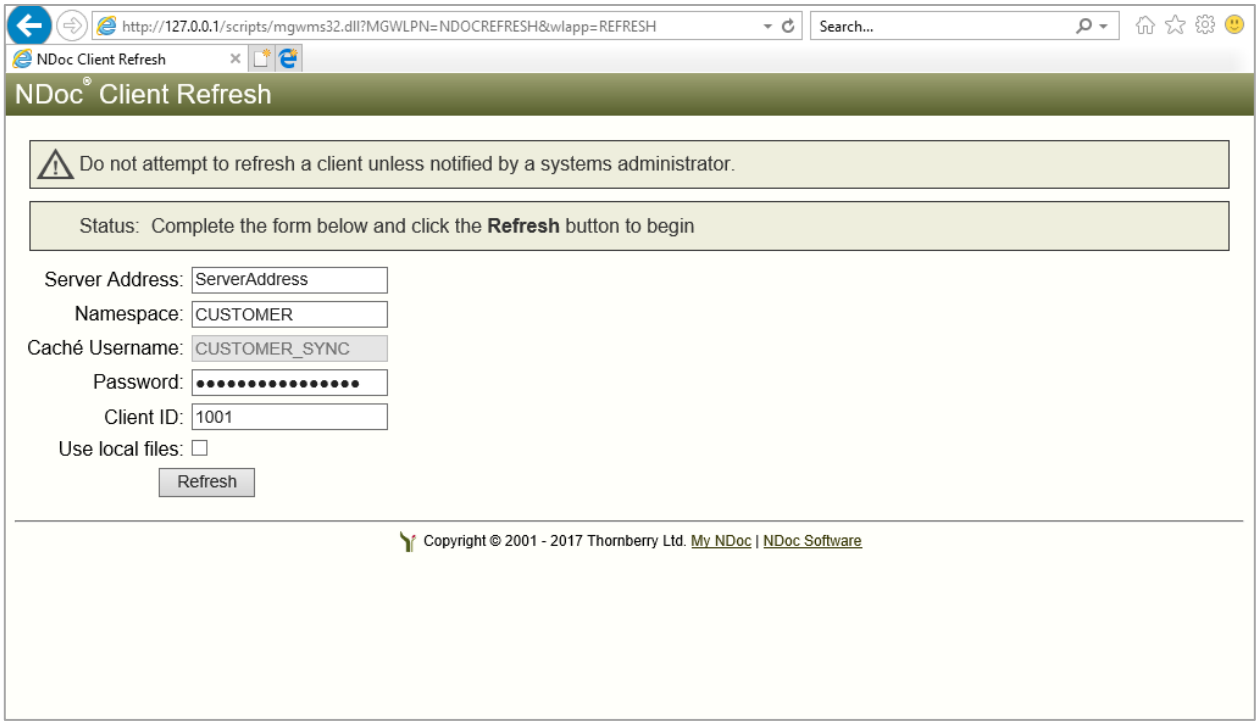
Although Caché is designed to prevent corruption, it is not unreasonable to expect corruption to occur within the device's Caché database through improper shutdowns or system crashes. When an event like this occurs, the refresh process can be utilized to save time and overhead of performing a full uninstall/reinstall of NDoc.

Another condition that comes up often is when a device is not synchronized to the server due to extended user absence, vacation, illness, etc., and has then passed file retention, causing an inability to synchronize and receive updates from the server. A refresh should be performed in this scenario to return the device to working condition before being returned to service.

To refresh a client:

1. Connect the client to a network as you normally would for synchronization.
   a. Connect any VPNs that you may need to use.
      Note: Customers hosted via the Thornberry's hosted solution, refer to the Hosted Customers section of the website for connection information needed.
2. Point the client's web browser to HTTP://127.0.0.1/clientrefresh.htm
3. Enter in the following information:
   a. Server IP Address or DNS name - refer to note below if unsure
   b. Namespace this client will be built from – refer to note below if unsure
   c. A valid NDoc login id for the namespace (Automatically populated based on namespace)
   d. The password for the login id ((found in Administration > System > Settings > Security)
   e. The 4 digit NDoc client ID assigned to the user of this client (assigned by NDoc System Manager under Administration>Employee>Assign Client Devices).
   f. "Use local files"is an optional check box. The refresh process uses three files built each night from the server to create the local instance of NDoc on the client. If left unchecked, the refresh process downloads the latest versions of these files from the server. If checked, usually for slower connections, the refresh uses the already manually downloaded files (explained on previous page) from the client.

Note: The Server IP and the Namespace are found in NDoc on the server in Administration > System > Settings > System (Client Devices > IP Address). Also, the fields in step a, b and e auto populate if this client has been refreshed before, but are blank if a new install. If a field has been auto populated but has an incorrect value edit it on the page (especially if client ID is incorrect).



4. Verify that you do want to "refresh" the client by clicking "OK" on the prompt that appears

Monitor the progress of the "refresh" periodically; checking for any errors. The message in the status box will update periodically to inform you of the progress. Error messages will also be displayed in this area.

Once the refresh has completed you will be redirected to NDoc sign-in page where you can log into NDoc. For the most accurate simulation of a local client in the field, you should log into both Windows and NDoc using the credentials of the employee to whom the client will be assigned.

Run a LAN-based sync first, then test a dial-up, then broadband if desired (these options are toggled by the radio button in Sync's 'Step 1'). For Step 2, select Daily Telephone Transfer, and then click Start.

Note: You are not required to complete both a dialup and broadband sync, but it is highly recommended that you test all options that will be accessed by the user.

Troubleshooting a Standalone/Local Client Refresh

This section contains some basic errors that might occur during refresh with some troubleshooting steps. When reporting these issues to the Thornberry Help Center sending us the text or screen capture of the error messages is always helpful.

Invalid Client ID

Verify that this client id currently exists on the server and that it is properly assigned to the correct user ID. Review the section *Creating or Changing the Standalone/Local Client Device ID*.

Server Error in Application "DEFAULT WEB SITE"

If this error occurs when browsing to the refresh page after completing the client installation process, then there was an issue with the installation of Internet Information Services (IIS) on the client. To correct this problem, log onto the client with a user that has administrative privileges and perform the following steps:

1. Open IIS on the client by Navigating to Start>Control Panel>Administrative Tools>Internet Information Services (IIS) Manager.

2. Click on the arrow next to the computer's name under the **Connections** section of the IIS Manager Window to have it expand.
3. Next click on the arrow next to **Sites** to expand this option.
4. Right-click on **Default Web Site** and then select **Manage Web Site>Advanced Settings** to bring up the Advanced Settings Window.
5. Change the **Application Pool** setting to "DefaultAppPool" instead of "LGXReports".
6. Change the **Physical Path** setting to "C:\inetpub\wwwroot" instead of "C:\inetpub\Scripts".
7. Click **OK** to save these changes
8. Restart IIS by clicking on the computer's name under the **Connections** section and then click **Restart** under the **Actions** section on the right hand side of the Window.
9. The problem should now be resolved and you should be able to navigate to the client refresh page.

The refresh webpage does not display

Make sure that http://127.0.0.1 is in the trusted sites and the Temporary Internet Cache is cleared.

Refresh takes a long time on a file (LIB, LIB_FDB, Tables)

If the refresh ends up not able to read the file and you are loading them down via the internet, sometimes there is an interruption in the communications between the PC and the server and this causes the file to not load properly on the PC. Simply start the refresh again and have it reloaded.

If you have the files located locally on the PC hard drive, they could be out of date or corrupted. Load down newer files from the server and put them into the C:\ndoc\restore\ folder. For instructions on how to download the files, refer to the File Downloads FASTForm.

If neither of these options work, please submit a request via the Thornberry Help Center.

Addendums

The following sections provide additional details on many of the processes and applications in use within NDoc.

Server Operations and Maintenance

This section is a guide to NDoc server operations. NDoc is built using the HealthShare and Caché database technology from InterSystems Corporation headquartered in Cambridge, MA. Intersystems is currently the worldwide leader in healthcare information database technology. This section focuses on an overview of the HealthShare and Caché software and continues into the details of how to perform maintenance tasks.

Introduction to HealthShare and Caché

The NDoc server utilizes the HealthShare database software, while the standalone/local clients are installed with Caché. HealthShare is actually an extension of the core Caché database technology. With HealthShare the core features of Caché are built upon to create a seamless business technology integration environment. Since the features of HealthShare are not required on the client machine, Caché is installed. For the purpose of explanation HealthShare and Caché are used interchangeably in the documentation below.

Caché is a full-featured database system; it includes all the features needed for running mission-critical applications (including journaling, backup and recovery, and system administration tools).

Running Caché

The primary Caché interface on Microsoft Windows platforms is the Caché Cube. From the Caché Cube, you can start all of the Caché configuration and management tools. You can also invoke each Cube command from a shortcut or command line.

Correspondingly, you can initiate many of the Caché tools from the Start menu by pointing to Programs, Caché, and then to the appropriate Caché instance name. When you start Caché on a Windows-based system, the Caché Cube  (or HealthShare icon) appears in the system tray of the taskbar. When you click the Caché Cube, a menu appears with commands to use the Caché utilities and programming environments. The following table describes some of the commands available from the Caché Cube menu.

Start Caché	Starts the default instance specified in the square brackets after the menu item, for example [CACHÉ]. If the Caché server is already started, this option appears dimmed—it is unavailable. For information about how to prevent an instance from starting automatically, see the *Memory and Startup Settings* section.
Stop Caché	Shuts down or restarts the local Caché instance. If the Caché server is stopped, this option appears dimmed—it is unavailable.
Terminal	Invokes the command line interpreter in the Caché programming environment
System Management Portal	Performs common system management tasks. Creates databases and namespaces, and adjusts all Caché configuration settings. Displays classes, globals, routines, and functions for managing each. Displays tables and views, perform queries and SQL management functions. See the *System Management Portal* chapter for more information
Preferred Server [server name]	Shows a list of remote servers and maintains server connections by using the Add/Edit command on the submenu. The preferred server appears in brackets and has a check mark next to it in the server list
Exit	Removes the Caché Cube icon from the system tray; this does not stop Caché

Starting, Stopping, and Restarting Caché

To start Caché, right-click on the Caché icon in the system tray and click Start. Similarly, to stop or restart Caché right-click on the Caché icon and click Stop. Two options are shown, Shutdown and Restart. Choose the applicable option and click Ok.

Alternatively, you can run commands in the "Run…" window (Start→Run) or in a Command Prompt.

Where <install-dir> is the directory in which Caché/HealthShare is installed:

To start the instance named NDOC, enter the following command at a command prompt.

```
start /wait <install-dir>\bin\css.exe start NDOC
```

To stop Caché from the command line use the following command at a command prompt.

```
start /wait <install-dir>\bin\css.exe stop NDOC
```

The previous commands can be used for scripting a shutdown and/or startup of Caché. For further reference on setting up a script to shutdown Caché/HealthShare, please refer to *Preventing Caché Database Startup Failures*.

When Caché is not running, the Caché Cube icon appears dimmed. If the Caché Cube is not in the system tray, from the Start menu point to Programs, Caché, the Caché instance name, and click Launcher.

Normally you leave your Caché system running. However, if your operating system requires a restart, stop Caché before you shut down your system. The Caché maintenance tasks, such as backups and database repair utilities, do not require you to stop Caché.

Note: If you have any trouble starting Caché, view the cconsole.log file located in the HealthShare or Caché installation directory. Thornberry support will often request this file for troubleshooting if there is an issue starting HealthShare or Caché.

System Management Portal

Caché lets you perform system administration and management tasks via a CSP application, the InterSystems System Management Portal (SMP). An advantage of this approach is that Caché does not have to be installed on the system you use to manage an installation. Remote management of systems over a network, subject to access control established for the site, is now much easier. Cross-release compatibility issues are minimized because both the data and its formatting information come directly from the system being managed.

To open the System Management Portal, enter the following address in your browser:

HTTPS://<server-address>:8972/csp/sys/UtilHome.csp

Memory and Startup Settings

When you first install NDoc with HealthShare/Caché, you may wish to change some default system information. The [Home] > [Configuration] > [Memory and Startup] page of the System Management Portal provides an interface to the database allocation features (memory performance settings), as well as a few startup settings:

1. You can choose whether to configure memory automatically or manually.

   If you choose *Manually*, you can specify how global buffer pool memory is allocated among 2-KB and 8-KB block sizes. These settings should be set to approximately 75% of the available RAM on the PC.

   If you choose *Automatically*, the system allocates the amount of memory best suited to Caché given the available memory. However, in some cases the memory settings will be adjusted much lower than what the system can handle and performance will be affected.

2. You can set your Caché instance to start automatically when the system starts by selecting the Auto-start on System Boot check box.

Note: The Auto-start on System Boot check box is selected by default. If you do not want the instance of Caché to start automatically on system boot, clear the check box.

3. If you are running in an IPv6 network, you can select the IPv6 Enabled check box to indicate that this instance of Caché accepts IP addresses in IPv6 format as well as IPv4 and DNS format.

   Note: The IPv6 Enabled check box is not displayed if the platform on which you are running Caché does not support IPv6 networking.

4. Click Save to save your modifications; restart Caché to activate them.

Some changes on this page require a Caché restart and some do not. If you modify one field that requires a restart, no change to your configuration takes effect until a restart, even those that normally do not require a restart.

Important: If you have made changes system-wide to the configuration settings that require a Caché restart, you receive the following:

WARNING: There are configuration changes saved that require system restart to take effect.

After you close the page, the warning message does not appear again to remind you that a restart is required.

Caché Backups

Since Caché is the most widely used database in healthcare today, and since healthcare sites operate 24x7, the Caché database includes a backup utility that backs up the database "on the fly" and enables nearly 24-hour availability of the database system.

Information systems integrity is the responsibility of the customer, although Thornberry can provide guidance.

Please note that Caché supports an advanced fail-over option called Server Shadowing. Shadowing requires additional hardware, but is particularly powerful. With server shadowing, each database server has a backup server that constantly reads the journal of the main server and updates the backup server's database. The backup server is useful for several purposes:

- In the event the main server fails, contact Thornberry for assistance to have NDoc up and running.
- The backup server can be used for reports and queries, offloading these tasks from the main server.

Server Shadowing is a software solution; there are other ways to promote fault tolerance such as disk mirroring and database clusters. These alternatives should be explored by the agency desiring ultimate protection for its database.

Principles of Caché Database Backup

A backup is a copy of the database at some instant in time. Should the physical integrity of the database be lost, the backup copy can be used to restore the database to the exact content that existed at the time of the backup, including all application data, security credentials, and transactions details.

You can think of each CACHE.DAT file as a separate or individual database. You also can think of your database as encompassing all of the CACHE.DAT files on your entire system. This larger body of data is what we mean by "your database" in this section.

A daily backup task is enabled with the NDoc installation for a subset of the full database list to generate a backup every morning at approximately 12:15am (actual time may vary by site). This backup includes all critical databases necessary for the restore of the NDoc application install and all pertinent data.

All Backups Are Concurrent

An important attribute of all Caché backups is that they can be performed while applications are running and the database is changing. To accomplish this, Caché backup employs multiple passes, as described in the following table:

Concurrent Backup Process	
First	The system keeps track of the blocks that are changed as the backup progresses.
Second and subsequent passes, except for the final pass	Blocks changed during the previous pass are backed up.
Final	At this point changes to the database are prohibited while the final set of blocks modified since the last pass are written out. During this phase application, users trying to modify the database pause momentarily. They resume execution when the last pass is complete.

Concurrent backup yields a snapshot of the entire database at one instant in time. That is, it copies the contents of all directories at the same point in time. The general-purpose backup facilities provided with most operating systems, which back up one file at a time, cannot provide such consistent and accurate backups.

For example, suppose you start a backup of three directories (A, B, and C) at 1:00 and it completes in thirty minutes. At completion, the backup reflects the contents of A, B, and C at 1:30. With other backup approaches, you might get a backup of A as of 1:10, B as of 1:20, and C as of 1:30. Whenever applications access multiple databases, such a backup makes further recovery nearly impossible. Caché backup avoids this dilemma.

Global Journaling Preserves Changes Since Last Backup

While a backup is the cornerstone of physical recovery, it is not the complete answer. Restoring the database from a backup makes the contents of the database current as of the time the backup was completed. Typically, this will be a long time (at least a number of hours) before the point at which physical integrity was lost. What happens to all the database changes that occurred since then? The answer lies with journaling.

Each computer running Caché keeps a journal. The journal is a file that keeps a time-sequenced log of changes that have been made to the database since the last backup. Journaling can be turned on for all modifications to the database, or it can be enabled selectively, on a global-by-global basis. Selective journaling avoids the overhead of saving updates to databases or globals for which recovery is not needed.

To recover databases from a loss of physical integrity, restore the backup and then restore the journal. Restoring the journal means reapplying the database changes from the journal. This technique is called "roll forward" recovery.

Internal Integrity Ensures Data Update Completion

Fortunately, with the high reliability of today's disk hardware, a loss of physical database integrity is relatively rare. Of more frequent concern is the threat to internal integrity. Internal integrity refers to the completion of an update that involves changes to more than one block in a database.

Updating the database involves three steps:

1. Getting the necessary blocks from disk into main memory, if they are not already there
2. Modifying the blocks in memory
3. Writing the blocks back to disk

The use of the plural "blocks" is important. A single database update may alter multiple blocks, and this presents opportunities for loss of internal integrity. Suppose, for example, that an update involves changes to three blocks. Suppose further that, because of an electrical power failure, two of these blocks are written to the database but one is not. Now the database is physically intact but internally inconsistent.

In reality the problem is even worse because database changes are not written immediately to the disk. Instead, changes are written periodically, on the order of every one to five seconds. This delay dramatically improves the performance by reducing the total number of disk writes. Updates tend not to be random. Rather, if a block is changed, there is a high likelihood that it will soon be changed again. By writing to the disk periodically, Caché accomplishes multiple changes to the same block with a single disk write.

Write Image Journaling

The solution to internal integrity threats lies in the use of write image journaling. This technology uses a two-phase process of writing to the database. Rather than writing directly from memory to the database, it uses an intermediate file, the write image journal, as follows:

Step 1:	All modified blocks are written to the write image journal.

Step 2:	All modified blocks are written to the database.
Step 3:	The write image journal is updated to indicate that step 2 completed successfully.

When Caché starts, it automatically checks the write image journal. If it indicates successful completion, the internal integrity of the database is intact. If not, the write image journal contains all of the information needed to complete Step 2 and return the database to a consistent state. This process is called *recovery*.

Recovery

The Caché recovery process has these important properties:

- First, it employs "roll forward" technology. In the event of a system crash, the recovery mechanism completes the updates that were in progress. By contrast, other vendors' systems employ a "roll back" approach, undoing updates to recover. While both approaches protect internal integrity, the roll forward technology used by Caché does so with reduced data loss.
- Second, Caché protects the sequence of updates. That is, if an update is present in the database following recovery, then all preceding updates are present as well. Other systems that do not correctly preserve update sequence may yield a database that is internally consistent but logically invalid.
- Third, the protocol protects the incremental backup files as well as the database. Thus, following recovery from a crash, a valid incremental backup can be performed.

Incomplete Updates

Note that, while the two-phase write protocol safeguards internal database integrity, it does not prevent data loss. If the system failure occurs prior to a complete write of an update to the write image journal, Caché does not have all the information it needs to perform a complete update to disk. Hence, that data will be lost.

Journaling

Overview

While a backup is the cornerstone of recovery, it is not the complete answer. Restoring the database from a backup does not recover changes made since that backup.

The Caché journaling function records changes made to the database between backups. The easiest way to employ journaling is to turn it on for all modifications to the database. (Journaling "all globals" is a standard NDoc configuration setting.)

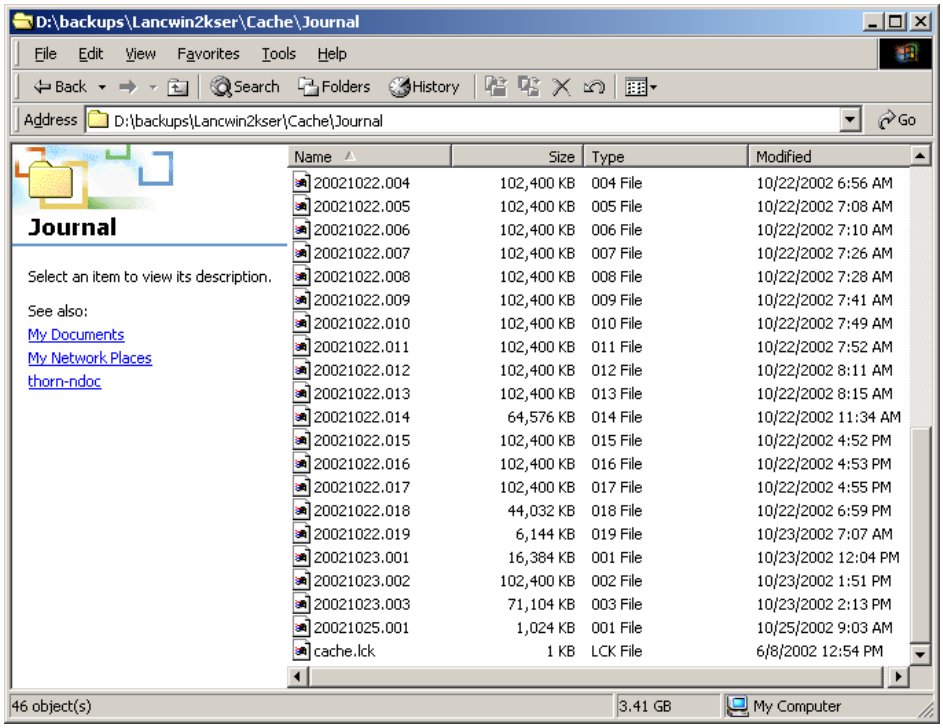
The journal provides a time-sequenced log of database activity. To recover from a loss of physical integrity, you restore the backup and then reapply the database changes from the journal. This method is known as "roll forward" recovery.

Journal Location

The location of journal files should be carefully selected to assure a full recovery in case of primary server failure. In other words, it is illogical to store journal files on the primary server since a failure of the primary server may likely require the restore of a backup and application of all subsequent journal files – and the latter would be on the failed machine!

Set the journal file location, and an alternate journal file location (in case the primary location is unavailable) in the Start Journaling (or Switch Journaling) dialog box depicted in the Start Journaling section, below.

A typical journal directory on a Windows server looks like this:



Each journal file uses the name construct *yyyymmdd.nnn* where *nnn* is a sequential number starting with 001 and incrementing by one upon rollover. A journal switch closes the active journal file, and begins a new *nnn*, regardless of whether the rollover was invoked manually or by NDOCBACKUP in conjunction with daily Caché backups.

The journal files in this directory are deleted each night by a scheduled task within the Cache database platform.

Restoring the Journal

After a system crash or disk hardware failure, you must recreate your database by restoring your backup copies. If you have been journaling and your journal file is still accessible, you can further restore your database by applying changes since the last backup, which have been tracked in your journal.

Caché Console Messages

Caché reports general messages, system errors, certain operating system-related errors, and network errors through an operator console facility.

For Caché systems, all console messages are sent to a log file in the system manager's namespace, \NDoc\Intersystems\mgr\cconsole.log. The console log file receives copies of all messages sent to the console terminal and stores them in a file. The log file is a plain text file and may be viewed with any editor or text.

Managing the Console Log File

Caché does not delete the log file. As system manager, you must review this file periodically, and remove it if it is too large. You can delete this file safely even when Caché is running, because Caché recreates it the next time there is a message to the log.

Sample cconsole.log Entries

Normal Journal Switch and Delete:

```
Caché (1044) Sat Aug 31 14:30:25 2002  CACHÉ JOURNALING SYSTEM MESSAGE
Automatic journal file roll to: d:\journal\20020831.005

Caché (2604) Sun Sep 01 00:15:01 2002  CACHÉ JOURNALING SYSTEM MESSAGE
Journaling switched to: d:\journal\20020901.001

Caché (2604) Sun Sep 01 00:15:01 2002  SWITCH: d:\journal\20020901.001

Caché (2604) Sun Sep 01 00:15:02 2002  DELETE: d:\journal\20020829.001

Caché (2604) Sun Sep 01 00:15:02 2002  DELETE: d:\journal\20020829.002
```

Normal shutdown: (extra linefeeds removed to save space in this document)

```
Caché (2792) Tue Sep 17 17:32:02 2002  Shutting down Caché
Caché (2792) Tue Sep 17 17:32:02 2002  Notifying Clients
Caché (2792) Tue Sep 17 17:32:02 2002  Executing user-defined shutdown routines
Caché (2792) Tue Sep 17 17:32:02 2002  Stopping User Jobs
Caché (2792) Tue Sep 17 17:32:02 2002  Stopping Network Server
Caché (2792) Tue Sep 17 17:32:02 2002  Stopping License Server
Caché (2792) Tue Sep 17 17:32:02 2002  Waiting for users to stop
Caché (2792) Tue Sep 17 17:32:03 2002  Stopping Client Networking
Caché (2792) Tue Sep 17 17:32:03 2002  Waiting for disk cleanup to finish
Caché (2792) Tue Sep 17 17:32:04 2002  Stopping Journaling
Caché (2792) Tue Sep 17 17:32:05 2002  STOP: d:\journal\20020917.011
Caché (2792) Tue Sep 17 17:32:05 2002  Stopping System Jobs
```

```
Caché (1076) Tue Sep 17 17:32:07 2002  Marked WIJ file as deleted
Caché (2792) Tue Sep 17 17:32:08 2002  Removing database locks
Caché (2792) Tue Sep 17 17:32:08 2002  Shutdown complete
```

Normal startup: (extra linefeeds removed to save space in this document)

```
*** Recovery started at Tue Sep 17 17:30:48 2002
    Current default directory: d:\ndoc\intersystems\mgr
    Log file directory: d:\ ndoc\intersystems \mgr\
    WIJ file spec: d:\ ndoc\intersystems \mgr\CACHE.WIJ
Recovering local (d:\ ndoc\intersystems \mgr\CACHE.WIJ) image journal file...
Starting WIJ recovery for 'd:\ ndoc\intersystems \mgr\CACHE.WIJ'.
 0 blocks pending in this WIJ.
Exiting with status 3 (Success)
Caché (0) Tue Sep 17 17:30:50 2002  No journaling info from prior system
Caché (1076) Tue Sep 17 17:30:53 2002
cstart of Caché for Windows NT (Intel) 4.1.3 (Build 175) Mon Dec 3 2001 16:22:28 EST.
          in d:\cachesys\mgr
          with wij: d:\cachesys\mgr\CACHE.WIJ
          from: d:\cachesys\mgr\
 OS=[NT], version=[5.0.2195], 2 processors.
 Processor type=[586], level=[6], revision=[2054], active processor mask=[3].
Caché (1076) Tue Sep 17 17:30:53 2002   System Initialized.  Write Daemon started.
Caché (1772) Tue Sep 17 17:30:58 2002  Performing Journal Recovery
Caché (1772) Tue Sep 17 17:30:58 2002  Nothing to restore from the journal
Caché (1772) Tue Sep 17 17:30:58 2002  Performing Transaction Rollback
Caché (1772) Tue Sep 17 17:30:58 2002  Processing Net section
Caché (1772) Tue Sep 17 17:30:58 2002  Processing License section
Caché (1772) Tue Sep 17 17:30:58 2002  Starting license server
Caché (1772) Tue Sep 17 17:30:58 2002  LMF info: License Server installed on address 127.0.0.1 port 4001
Caché (2048) Tue Sep 17 17:30:58 2002  LMF info: License server failover is not configured.
Caché (1772) Tue Sep 17 17:30:58 2002  Processing Datasets section
Caché (1772) Tue Sep 17 17:30:59 2002  ...d:\ ndoc\intersystems \mgr\cachetemp\ initialized as CACHETEMP
Caché (1772) Tue Sep 17 17:30:59 2002  Processing Namespace section
Caché (1772) Tue Sep 17 17:30:59 2002  Processing CSP Applications section
Caché (1772) Tue Sep 17 17:30:59 2002  Starting Network
Caché (1772) Tue Sep 17 17:30:59 2002  Activating Namespaces
```

```
Caché (1772) Tue Sep 17 17:31:00 2002  Now translating dataset names
Caché (1772) Tue Sep 17 17:31:00 2002  Now activating namespace configuration CACHÉ
Caché (1772) Tue Sep 17 17:31:01 2002  Namespace configuration CACHÉ has been activated
Caché (1772) Tue Sep 17 17:31:01 2002  DCP Server enabled
Caché (1772) Tue Sep 17 17:31:01 2002  Processing Language section
Caché (1772) Tue Sep 17 17:31:01 2002  Processing Locale Information
Caché (1772) Tue Sep 17 17:31:01 2002  Processing Startup section
Caché (1772) Tue Sep 17 17:31:01 2002  Max Journal Size: 104857600
Caché (1772) Tue Sep 17 17:31:01 2002  START: d:\journal\20020917.011
Caché (1772) Tue Sep 17 17:31:03 2002  Journaling all globals to d:\journal\20020917.011 started.
Caché (1772) Tue Sep 17 17:31:03 2002  Processing Devices section
Caché (1772) Tue Sep 17 17:31:03 2002  Loading custom device mapping tables ...
Caché (1772) Tue Sep 17 17:31:03 2002  Processing DeviceSubTypes section
Caché (1772) Tue Sep 17 17:31:03 2002  Processing MagTape section
Caché (1772) Tue Sep 17 17:31:03 2002  Processing IO section
Caché (1772) Tue Sep 17 17:31:07 2002  Processing SQL section
Caché (1772) Tue Sep 17 17:31:07 2002  Processing CSP section
Caché (1772) Tue Sep 17 17:31:07 2002  Processing SQL Gateway Connections section
Caché (1772) Tue Sep 17 17:31:07 2002  Processing Miscellaneous section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Lat section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Telnet section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Com section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Netbios section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Shadowing section
Caché (2380) Tue Sep 17 17:31:07 2002  Processing Viewpoint section
Caché (2380) Tue Sep 17 17:31:07 2002  Purging old application errors
Caché (1772) Tue Sep 17 17:31:07 2002  Enabling logons
```

Errors that may be logged in cconsole.log

Journaling not started

A “Write to journal file failed” entry in cconsole.log may mean the drive connection to the journal location has disappeared, or the journal location’s disk is full, and journaling cannot start. Check disk space and drive mapping, restart Caché and check for errors.

Disk has run out of space

The “diskfull” error means Caché has attempted a write to a full disk. This is generally caused by failure to properly maintain journal or backup files. Delete unnecessary backup (.cbk) files and/or old journal files (any older than the last good backup are safe to delete), restart Caché and check for errors.

Disk cannot be written to

The “diskhard” error usually signifies an attempt by Caché to write to a file that has been locked by another process. This is common in tape backup scenarios (Arcserve, etc.) where the tape utility has not been told to bypass the \ ndoc\ directories. The backup utility should backup the \journal\ and \backup\ (folder containing the Caché .cbk backup files) rather than attempting to backup the functioning Caché environment.

This error has also been encountered when virus scans lock Caché database files (CACHE.DAT’s) that have already been mounted (are in use by NDoc).

Web Server Configuration

Web services (IIS) are configured during NDoc installation and generally require no further tuning. However, web services event logging in Windows can consume significant disk space over time and should be monitored by the systems administrator.

Disaster Recovery

Every business needs its own disaster recovery plan and method for backing up and restoring data needed from NDoc in the event of a disaster. This document describes the items that your agency should take into account as you plan your disaster recovery methodology.

Virtual Machine Considerations

NDoc and Healthshare is well suited to run on virtual machines, and have proven its stability over the years in that configuration. With most servers being virtualized, backup methodology has improved to be more efficient. Nowadays most agencies have a backup method where a snapshot of the full virtual server, as a state in time picture of the operating system, as well as the state of the applications running on that server.

We have worked with Intersystems to develop scripts that should work with your snapshot backup software. It is highly recommended that all agencies using virtual machine snapshots work with Thornberry to implement these scripts, as well as the necessary database configuration. These scripts work with Intersystems' own code base to set the databases up to be quiescent before the snapshot is taken, providing your technical team piece of mind that the snapshot will contain clean backups of the Healthshare databases.

The first script is a "pre-freeze" script, that is setup to execute by the backup software before it freezes the virtual machine, so that Healthshare will pause writing to the database files until it is given the thawing command. The second script is a "post-thaw" script, which sends the thaw command to Healthshare, releasing the hold that the application was performing for writing data out to the database files.

Both of these scripts are customized to your agencies specific NDoc installation, and can be made available for review before or after their implementation. When your agency is ready to implement this configuration, a Thornberry technician will need to perform configuration work on the Healthshare instance to allow these scripts to run properly and under minimum permissions to your instance. In fact, the credentials created for the backup procedures only have one permission - to run the freeze and thaw commands.

File Based Considerations

By default, in a new installation, Healthshare is configured to run a file based backup of all the databases on the server. This file is saved as a CBK file, and normally the last 2 days of this file are kept on the server. The CBK file will continue to grow in size as data is added to your NDoc instance. The latest version of this file is just one of the pieces of data that would be needed in the event of a disaster recovery. In a file based backup scenario, if the server would go down and become unrecoverable, we would need to rebuild the NDoc server instance on a new (or rebuilt) server machine.

Important: The HealthShare journal directory listed below can (and should) only be backed up if the backup method or software does not have the ability to backup the most recently edited file. The file with the most recent modified timestamp is the journal file in current use. Locking this file for backup while the HealthShare database software is attempting to edit it will cause the system to freeze writing to the disk, i.e., HealthShare will not resume normal operation.

Item	Description	Location
HealthShare Database Backup	Backup of all HealthShare Database files. Multiple days of files may exist depending on backup settings.	<HealthShareBackupDirectory>*.cbk

HealthShare Journal	HealthShare journal files contain database transactions created since the last database backup was taken.	\Journal*.*
IFACE (Interfaces)	Various interface related files for NDoc. Can be located on another server or on two separate servers depending on your setup.	\IFACE*.*
SFTP	Standalone/local client synchronization files, including visit charting from the local clients, update installation files for the local clients, and more.	\Comm*.* or \NDoc\FTP*.*
NDoc	All utilities, temporary interface files, reports (and reporting engine), and other misc. files for NDoc. Includes NDoc related files that are stored externally from the HealthShare databases, including items like wound photo files.	\NDoc*.*

Backup File Exclusions

Due to the nature of how database software operates, some file exclusions may need to be added to the backup method chosen to avoid locking any of the HealthShare database files while they are in use. Though it is not necessary to backup the contents of the \NDoc\Intersystems\ directory, you may include this directory (e.g. full drive/system backup). If your backup locks files while backing up and targets any of the following files, then these files must be added to the backup exclusion list to prevent issues with writing to database files while in production:

\NDoc\cache.dat

\NDoc\Agencies\<SITENAME>\patient\cache.dat

\NDoc\Agencies\<SITENAME>\audit\cache.dat

\NDoc\Agencies\<SITENAME>\cache.dat

\NDoc\lib\cache.dat

\NDoc\lib\fdb\cache.dat

\NDoc\temp\cache.dat

\NDoc\Intersystems\mgr\cache.dat

\NDoc\Intersystems\mgr\cachelib\cache.dat

\NDoc\Intersystems\mgr\cachetemp\cache.dat

\NDoc\Intersystems\mgr\ensemble\cache.dat

\NDoc\Intersystems\mgr\enslib\cache.dat

\NDoc\Intersystems\mgr\CACHE.WIJ

The HealthShare journal directory listed below can (and should) only be backed up if the backup method or software does not have the ability to backup the most recently edited file. If this ability is not possible then the directory as listed below must be excluded completely. Backing up this file set while the HealthShare database software is attempting to edit one of them will cause the system to freeze writing to the disk, i.e. HealthShare will not resume normal operation.

\Journal*.*

Disaster Recovery Steps (Virtual Machine Snapshot)

In the event of a disaster, the steps you will need to perform are listed below. Due to the amount of tasks that could or could not be needed in order to fully restore all data, always contact Thornberry support for assistance in disaster recovery. If it is after hours, contact Thornberry emergency support.

1. Restore the server virtual machine to the last snapshot taken.
2. Confirm that the server operating system loads as expected.
3. Ensure remote access for Thornberry support.
4. Contact Thornberry support. A Thornberry support representative will update you with a status at any time.
5. When the recovery is completed, a Thornberry support representative will contact you to allow user-side testing:
    a. Test synchronization from a local client.
    b. Test login from a workstation client.
    c. Test proper loading of all top-level modules (Care Pilot, Medications, Orders, etc.).
    d. Test proper loading of reports.
    e. Test 485 Preview.
    f. Test 485 Reprint.
6. Any vendors providing interfaces that need to be contacted to restart the interface on the vendor side can be done now.

.

Overview of Thornberry Procedures (Virtual machine snapshot)

The following steps will be performed by Thornberry support representatives, depending on the state of the virtual machine after the restoration from the snapshot backup is completed.

1. Confirm that Healthshare has started back up properly
    a. If Healthshare does not start properly, Thornberry will troubleshoot the startup errors, escalating to Intersystems support if necessary to resolve
2. Confirm that Healthshare productions start properly, including all production interfaces that the agency has enabled.
3. Confirm that the Java Grouper is processing properly
4. Confirm that Thornberry Support is able to log into NDoc.
    a. Test proper loading of all top-level modules (Care Pilot, Medications, Orders, etc.).
    b. Test proper loading of reports.
    c. Test 485 Preview
    d. Test 485 Reprint
5. Confirm that the system's SFTP server is running as expected; test connectivity to SFTP server if possible

Disaster Recovery Steps (File based backup)

In the event of a disaster, the steps you will need to perform are listed below. Due to the amount of tasks that could or could not be needed in order to fully restore all data, always contact Thornberry support for assistance in disaster recovery. If it is after hours, contact Thornberry emergency support. The disaster recovery process, involving a full server rebuild, is estimated to take approximately 6-8 hours, though it is highly dependent on the exact nature of the disaster and what needs to be recovered.

1. Transfer all files listed in the Disaster Recovery File List section from the backup medium being used to a location directly accessible from the server where the data is to be recovered.
2. If the new target server for the restore replaces the former, then the IP address on the LAN must be the same as the previous server for connectivity from workstation and local clients. Make any necessary changes to ensure this now.
3. Ensure remote access for Thornberry support.
4. Contact Thornberry support. A Thornberry support representative will update you with a status at any time.
5. When the recovery is completed, a Thornberry support representative will contact you to allow user-side testing:
    a. Test synchronization from a local client.
    b. Test login from a workstation client.
    c. Test proper loading of all top-level modules (Care Pilot, Medications, Orders, etc.).
    d. Test proper loading of reports.
    e. Test 485 Preview (confirms Apache is running).
    f. Test 485 Reprint (confirms Apache is running).
6. Any vendors providing interfaces that need to be contacted to restart the interface on the vendor side can be done so now.

Overview of Thornberry Procedures (File based backup)

In the event of a disaster, the steps you will need to perform are listed below. Due to the amount of tasks that could or could not be needed in order to fully restore all data, always contact Thornberry support for assistance in disaster recovery. If it is after hours, contact Thornberry emergency support. The disaster recovery process, involving a full server rebuild, is estimated to take approximately 6-8 hours, though it is highly dependent on the exact nature of the disaster and what needs to be recovered.

Note: The steps described below are followed if the server running NDoc has become unusable through a disaster and requires data restoration from backups.

1. Verify the following necessary data is available.
    - \ndoc*.*
    - \ndoc\docs*
    - \ndoc\Backup*
    - \ndoc\FTP* (or \comm*)
    - \ndoc\utilities*
    - \ndoc\web*
    - \IFACE*
    - \ndoc\Intersystems\mgr\journal*.*

    Note: Journal files are only applied if created after the backup completion time.
2. If any shadow servers are present, stop shadowing service before rebuild of primary.
3. Perform a new production server setup taking into consideration the files that have been restored. This mimics a server migration.
    - \ndoc\web*
    - \ndoc\utilities*
    - \ndoc\Backup*
4. Restore HealthShare and customer databases:
    - Agency database
    - Agency Patient database

- Agency audit database
- LIB (only if versioning differences)
- LIB_FDB (only if versioning differences)
- Main application database - \Ndoc\cache.dat

5. Restore journal files if they exist and were created after the completion time of the backup.
    - Copy \ndoc\intersystems\mgr\journal* files to location on production server.
    - Run the journal restore utility.
6. Restore files used for operations such as synchronizations, then place them in the correct location.
    - \ndoc\docs*
    - \ndoc\FTP* (or \comm*)
    - \IFACE*
7. Check of interfaces to ensure operability.
8. If nightly processing has not completed, run the process to completion.
9. Ensure functionality of all major NDoc application components.
10. Test synchronization of a local client (assuming appropriate access is available).
11. If any shadow servers are present and were not failed over to already (see the Shadow Server Failover section):
    - Run primary backup routine on restored server.
    - Copy backup from production server to shadow server.
    - Restore databases to shadow server:
        - Agency database
        - Agency Patient database
        - Agency audit database
        - LIB
        - LIB_FDB
        - Main application database - \Ndoc\cache.dat
    - Copy updated non-Healthshare files to shadow server:
        - \ndoc\docs*
        - \ndoc\FTP* (or \comm*)
        - \ndoc\web*
        - \IFACE*
    - Confirm that all databases are setup in the shadowing configuration.
12. Restart shadown service, starting from checkpoint right after backup

Troubleshooting User Access

If the user has issues after logging into NDoc accessing certain areas of the software or there are issues accessing user IDs or an issue with IDs being locked out these sections cover these areas.

Common questions and answers

- After you assign a team in Discipline Referral, there are no employee names to select even though I entered all our NDoc users into ID Maintenance.
  Employee names appear under team listings when the employee is assigned to a team in the ID Maintenance function. In addition to assigning a User Type, you must also assign a team. An employee may be on more than one team in this table.

- Our teams are set up and employees are assigned correctly, however the employees are advising that they can only assign one TEAM member in Discipline Referral. What can we do?
  When you need to assign clinicians from the same TEAM to a patient, you will use the 'Assign Patient to User' function. You may assign any number of clinicians to patients from this function.

- I want to prevent certain departments from having access to NDoc. I thought that this was already set up. Is there a reference for me?
  Yes, you can first review a listing of the assigned functions by User Type in Administration/Employee/User Type Access. This table display will confirm what functions are currently assigned by User Type. You may uncheck any function, which then removes access to the function for that User Type.

- I have an employee whose job responsibilities don't appear to be met by the current NDoc User Access table. I used a standard User Type, but now it appears this will not work. I have to limit function access. What do I do?
  First, you'll want to create a new User Type. Doing so will allow you to 'define' this particular employee's NDoc access. User Type is set up in ID Maintenance, where you'll select Add, enter the name of this User Type, make sure you check ACTIVE, assign a team if needed and then Save. Now you can go to the User Type Access table and simply 'check' the NDoc functions you wish to assign to your new User Type. This process defines an agency-specific user type as well as that user type's NDoc access.

- *I have users who have forgotten their passwords or have gotten locked out? What do I do?*
  If a user forgets their password or if the rule for locking out a user is active and a user becomes locked out because they or someone else tried too many times, the steps to follow are determined by whether the user logs in directly to NDoc via a workstation or is an NDoc standalone/local client user.

  Forget password and user logs in at server

  a. Sign on as System Manager on the server.
  b. Access Employee\Employee Table\Access and retrieve the employee.
  c. Assign a new (temporary) password in the Password field, check the box to require a user to change their password and save the changes.
  d. Have the user log in and change their password.

  User locked out or gets message access denied and logs in at server

  a. Sign on as System Manager on the server.
  b. Access Employee\Employee Table\Access and retrieve the employee.
  c. Make the user Active again clicking OK to the message boxes. This clears out the lockout attempts.
  d. Assign a new (temporary) password in the Password field, check the box to require a user to change their password and save the changes.

e. Have the user log in and change their password.

Forget password and user accesses NDoc from local client

a. Sign on as System Manager on the server.
b. Access Employee\Employee Table\Access and retrieve the employee.
c. Assign a new (temporary) password in the Password field, check the box to require a user to change their password and save the changes.
d. Have the user log in to the client with an administrative login such as SYSMAN.
e. Have the user sync and the new password is brought down to the client.
f. Have the user log out of SYSMAN and log in with their ID changing their password.
g. The user should then make sure to sync after charting is completed to ensure the updated password is transferred back to the server.

User locked out or gets message access denied and accesses NDoc from local client

a. Sign on as System Manager on the server.
b. Access Employee\Employee Table\Access and retrieve the employee.
c. Change the user from Active to Inactive back to Active clicking OK to the message boxes.
d. Assign a new (temporary) password in the Password field, check the box to require a user to change their password and save the changes.
e. Have the user log in with an administrative login such as SYSMAN onto their client.
f. Have the user sync and the user's account is made active, the lockout attempts are cleared, and the new password is brought down to the client.
g. Have the user log out of SYSMAN and log in with their ID changing their password.
h. The user should then make sure to sync after charting is completed to ensure the updated password is transferred back to the server.

User/Patient Record Locks within NDoc

In order to maintain the integrity of the NDoc databases, patient and many other types of data records are locked while the data is in use to prevent another user or system process from accessing and possibly editing that data while it is still in use. In many cases, you receive a message that a certain user is in the record.

In the event that an NDoc session crashes or internet connectivity is lost, locks could remain on both patient records and an employee ID. Due to the way the database works to prevent data corruption, it removes the locks approximately 20 minutes afterwards. To allow users back into the software more quickly there is a Reset User function for the server detailed below. On a local client, steps are provided below as well for the user to gain access more quickly. If an ID or patient record remains locked after trying these steps or 20 minutes has passed please submit a request via the Thornberry Help Center.

On the server

A user login may be reset by a Systems Manager as shown below.

Using the Reset User function

1. Access via Administration > System > Dashboard.
2. Select the user ID that is locked from the drop down list and click the Reset User button.

   WARNING: All user IDs are displayed in this function and resetting a user that is not locked will cause data loss.
3. Once the user is reset, they can login.

On the NDoc client installed device

The user can try two things:

- Once exited from NDoc, they should exit IE and then reenter IE and try to login again.
- If the above does not allow re-entry or the patient record is still locked, then the user should reboot the PC which should clear all locks from the system since the NDoc Cache database is restarted.

Recover Charting from Local Client that Cannot Synchronize

This procedure is used to recover charting from a local client where the synchronization is failing. The usual cause of such a failure is a database integrity problem rendering the synchronization function inaccessible or useless due to <SYNTAX> or <DATABASE> or <RUNTIME> errors. **Charting must be recovered from the failing client before rebuilding/refreshing. Failure to do so will require the clinician to re-enter their data.**

This procedure must be run by the NDoc system manager and presumes the system manager has a working knowledge of how to open and use Caché Terminal, and has the appropriate Windows permissions to move flat files from clients to the Caché server.

Recovery Steps

On the failing client:

1. On the client, right-click on the Caché cube in the system tray (located in the lower right corner of your screen, you should see a blue cube), and select "Terminal" to open a terminal session.
2. Type zn "NDOC" and hit <Enter>; it should have the NDOC> prompt when done.
3. At the prompt, type d ^qSAVECHARTINGDATAONLAPTOP and hit <Enter> to generate the file c:\comm\recover.dat, which will have the charting in it.
4. At the NDOC prompt, Type H and hit <Enter> to close the terminal session on the client.

   You need to move the recover.dat file off the client to the NDoc server using the network or putting it on a thumb drive or burning it onto a CD.
5. Transfer the file to the server into the Y:\COMM\XXX\NNNN\ subdirectory, where Y is the drive where the COMM folder is usually located (usually C or D); XXX is the company name or abbreviation; NNNN is the client ID (you can get this from Administration>Employee>Assign Client Devices).
6. On the NDoc server, right-click on the HealthShare cube, and select "Terminal" to open a terminal session.
7. Type zn "XXX" and hit <Enter>, where XXX is the company name/abbreviation. It should say XXX> when done.
8. At the prompt, type d ^qRECOVERCHARTINGDATAONSERVER and hit <Enter>.
9. When prompted, enter the client's 4-digit number and hit <Enter>.

   It will look in the folder, find recover.dat, read it in, and then do a "process patient now" on all the patients in the file so their charting will be posted into their charts immediately.
10. At the XXX> prompt, type H and hit <Enter> to close the terminal session on the server.

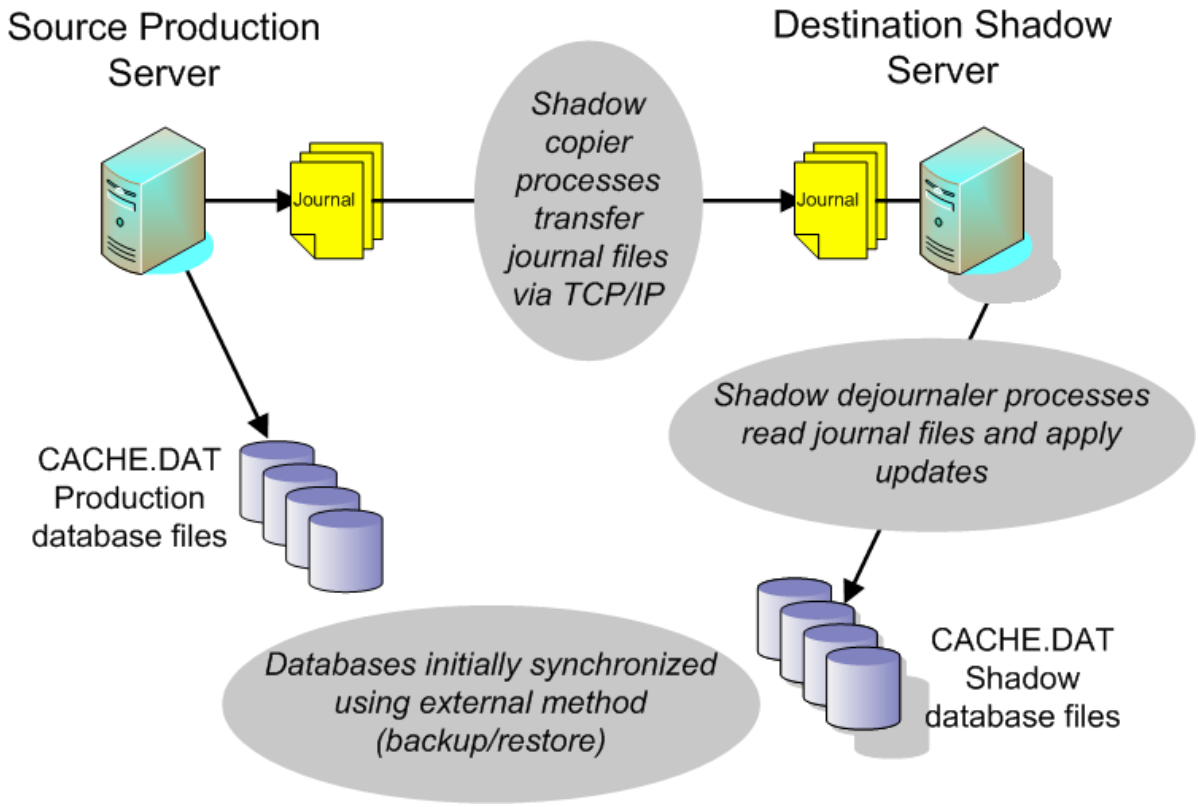
How it works

Charting will be recovered from both the NDOC namespace and any charting in pending communications flat file. If there is no charting to recover, the program will notify its user that only logs are being placed in the recovery file. The recovery programs will list patient names and account numbers being recovered. On the server, as soon as qRECOVERCHARTINGDATAONSERVER is run, processing is forced for all patients whose charting is in the recovery file. This means the recovered data will appear in the database immediately, unless someone is charting on a patient on a workstation. In that case, unless someone forces processing using the Process Patient Now function, the recovered charting will be saved until nightly processing.

Shadow Servers

Any NDoc setup has the option of adding one or more shadow servers. For NDoc a shadow server can serve two primary roles; one is to act as a reporting server and the second is for failover in a disaster recovery scenario. Shadow journaling monitors database activity on a primary system, the source, and causes the same activity to occur on a secondary system, the destination. It does this through a shadow client service running on the destination that continually requests journal file details from a shadow service running on the source. The shadow service responds by sending the details of the transaction, as it is recorded in each journal entry, to the destination shadow over a TCP connection. The source and destination servers can be of different hardware, operating system, or CPU chipset.

Shadowing Overview



All shadowing uses a fast transmission method which allows more efficient performance by sending the compacted journal file block by block. The shadow applies all transactions to the local databases. The transmission mode requires the data to be written to the journal file, which may introduce a delay of a few seconds. The shadow establishes a TCP connection to the server and receives the journal file. As the journal file downloads, another shadow process applies the journal entries to the local destination copy of the database.

Upon connecting to the data source server, the destination shadow sends the server the name of the journal file and the starting point. The shadow checks for new records periodically. If it does not have the latest records, the shadow downloads them and updates the databases. During these processes, Caché continually stores checkpoints in a shadow global to facilitate rollback and restart capabilities.

Caché purges the destination shadow copies of source journal files automatically. You can configure how long to keep files that are eligible for purging, that is, ones that have been dejournaled and do not contain any open transactions. This is defaulted to 3 days during the initial NDoc setup, but can be changed at any time.

As a Reporting Server

With a shadow server in place, reporting tasks will be offloaded to it to allow faster performance of other NDoc operations on the primary server. If multiple shadows are in place only one will be chosen to be the primary reporting server.

Shadow Server Failover

In the event of a disaster, where the primary NDoc server is lost, the shadow server may be failed over to and used for continuing NDoc operations. This allows for a more expedient recovery of the NDoc system as compared to a full NDoc server rebuild (as outlined in the *Disaster Recovery* section).

Due to the amount of tasks that could or could not be needed in order to fail over to the shadow server, always contact Thornberry support for assistance in disaster recovery. If it is after hours, contact Thornberry emergency support. Once Thornberry support has been contacted the process of performing the failover is estimated to take approximately 1-2 hour(s), barring any unforeseen conditions that may occur. If Thornberry support estimates/evaluates the failover process to take any more than two hours to complete, you will be contacted immediately with an update on the conditions prohibiting completion within the estimated window of time.

Caché Controller Service Configuration

Depending on the agency's group policies on the domain, Caché may need administrative powers in order to successfully complete a number of background processes (e.g. an automated A.M. synchronization). If you are unsure if your agency needs to complete this step, then you should skip this step and come back to it if problems are encountered while trying to complete the automatic A.M. synchronization or while configuring Windows encryption (optional). To grant the *Caché Controller for NDOC* service Administrative powers, complete the following steps:

1. Right-click on 'My Computer' and select 'Manage'.
2. Expand 'Services and Applications' and double click on 'Services'.
3. Right click on the *Caché Controller for NDOC* service and select 'Properties'.
4. Select the 'Log On' tab at the top and then check the 'This Account' radio button (Image 1.18).

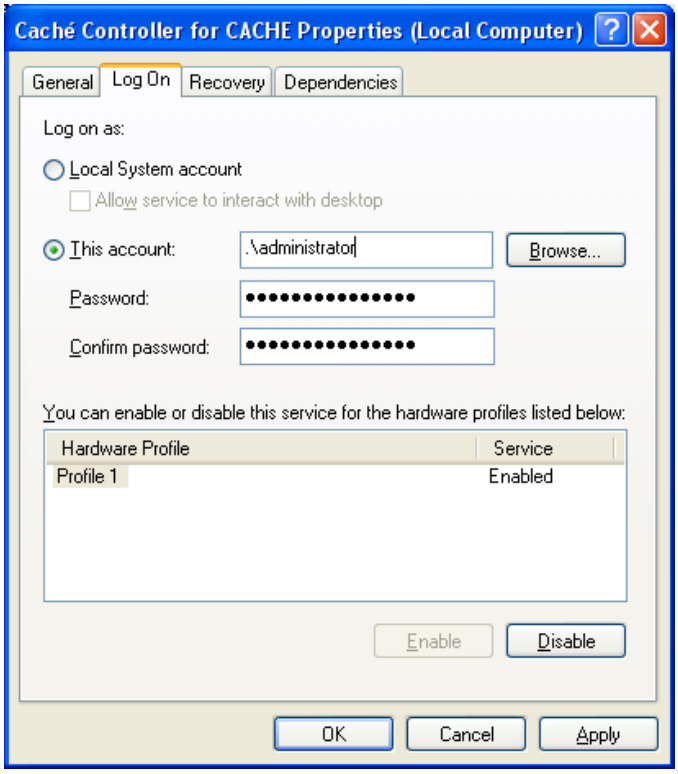


Image 1.18

Note: The password should be a non-expiring password or else it will need to be updated on the client every time the password expires.

5. Press ok and restart the *Caché Controller for NDOC* service.

Preventing Caché Database Startup Failures

Due to the nature of how database software operates (Caché/HealthShare for the purpose of this discussion), the best practice is to always shutdown the database software on the computer (client or server) prior to shutting down the operating system on the computer. When the operating system, in this case Windows, is shut down prior to the database software, the operating system sends a message to the database software of its intention to shut down. The problem with this is that the operating system does not know or care whether or not the database software has any of its own processes running currently. The database software is then forced to do a quick shutdown, thus killing any open processes as quickly as it can without losing information.

All of the processes related information (transactions), at the time the processes were closed prematurely, is contained in a file called the write image journal (WIJ) file for it to be able to recover any unsaved information through a process called journaling. This information itself in the WIJ file can become corrupt depending on the timing of when the database software was forced down, which in turn causes an issue with the startup of the databases when trying to journal the information in the WIJ file. However, the majority of startup issues come from the case where the computer (client or server) was shut down outside of the operating system (loss of power, etc).

The best way to prevent startup failures with the Caché/HealthShare database software is to create a script that will get run whenever the client or server is shutdown. The script's purpose is to force the operating system to wait for the database software to shut down before continuing with the shutdown fully. We provide a premade shutdown script that can be found under the Installation Files section after logging in at www.thornberryltd.com.

Implementing a Shutdown Script for NDoc

To implement a shutdown script that will stop the Caché/HealthShare database software properly during the operating system shutdown, complete the following instructions. If you would like to deploy this via a domain group policy, then only perform step 1 and consult the IT staff in charge of group policy deployment within your company.

1. Download the shutdown script, **NDocShutdown.zip**, from **HTTPS://www.ndocsoftware.com**. You must first login to the client access portion of the website. The file can be found under the section *Welcome >Installation Files > Installation Files* titled **Caché/HealthShare Shutdown Script**.
2. Extract the **NDocShutdown.zip** file to a location that can be reached from the computer you are implementing the script for. The only file contained in the zip file should be **NDocShutdown.bat**.
3. The remaining steps need to be executed from the computer you are implementing the script for.
4. Open the '**Run…**' window (Start icon→Run).
5. In the '**Run…**' window type: **gpedit.msc**
6. The **Group Policy** window will now open. Navigate to **Computer Configuration→Windows Settings→Scripts (Startup/Shutdown)**, and then open the **Shutdown** item.
7. In the **Shutdown Properties** window click the '**Show Files…**' button and copy the '**NDocShutdown.bat**' file you extracted earlier in these steps to the folder that has opened up.
8. In the **Shutdown Properties** window click '**Add…**'.
9. In the **Script Name** field type: **NDocShutdown.bat**
10. Click OK.
11. Click OK again on the **Shutdown Properties** window.
12. Close the **Group Policy** window.

Troubleshooting a Caché Startup Failure

Below are some steps that can be done when troubleshooting a Caché/HealthShare startup failure. These steps are designed to help resolve common issues or narrow it down further. These steps do not cover all possible startup issues. If these steps do not help to resolve a startup issue, submit a request about your issue via the Thornberry

Help Center. Once any startup issue is resolved, it is highly recommended to perform the steps in the section *Implementing a Shutdown Script for NDoc* described above to help prevent startup issues from occurring again.

Check for any service logon errors

Open event viewer on the computer and check for any events that describe a logon error with the Caché Controller for NDOC service. Resolve the issues accordingly. In most cases the service should be set to logon as the default SYSTEM account in Windows.

Clear the Caché Write Image Journal

Sometimes Caché's write image journal file will become corrupt during a forced shutdown. Delete the file C:\ndoc\Intersystems\mgr\CACHE.WIJ and attempt to start Caché normally from the cube to correct any corruption in the write image journal.

Clearing out Caché journal information

Note: The paths for Caché/HealthShare may differ throughout these instructions depending on the location of your Caché/HealthShare installation.

Open the Caché log file, C:\ndoc\Intersystems\mgr\cconsole.log. If the file contains the following text at the end of the file then perform the rest of the steps below:

"Enter Caché' with C:\ndoc\Intersystems\bin\cache -sC:\ndoc\Intersystems\mgr -B and D ^STURECOV for help recovering from the errors. "

1. At a DOS command prompt execute the special commands indicated in these instructions to enter Caché/HealthShare:

   ```
   C:\ndoc\intersystems\bin\cache -sc:\ndoc\intersystems\mgr -B
   ```

   This runs the Caché executable from the Caché installation bin directory (*install-dir***\bin**) indicating the pathname (by using the **-s** argument) of the system manager's directory (*install-dir***\mgr**) and inhibits all logins except one emergency login (by using the **-B** argument).

2. You are now in the manager's namespace of the Caché instance and can run the startup recovery routine. To do this, enter the following command:

   Do^STURECOV

   The journal recovery menu appears (*see image 1.1 on the next page*).

3. Enter choice 8 and press the Enter key. When prompted to confirm, enter **Yes** to continue. For all other prompts you can hit the Enter key to accept the default option.
4. Once you arrive back at the menu (see image 1.1), enter choice 3 and press the Enter key. When prompted to confirm, enter **Yes** to continue. For all other prompts you can hit the Enter key to accept the default option.

   Caution: Only use the **^STURECOV** utility when you are experiencing a startup issue. Using it while the system is in any other state (for example, up running normally) can cause serious damage to your data, as it restores journal information if you ask it to and this information may not be the most current data. The **^STURECOV** utility warns you, but it lets you force it to run.

Journal Recover Menu

```
Journal recovery options

------------------------------------------------------------
```

```
1) Display the list of errors from startup
2) Run the journal restore again
3) Bring down the system prior to a normal shutdown
4) Dismount a database
5) Mount a database
6) Database Repair Utility
7) Check Database Integrity
8) Reset system so journal is not restored at startup
10) Display Journaling Menu (^JOURNAL)
------------------------------------------------------------
H) Display Help
E) Exit this utility
------------------------------------------------------------


Enter choice (1-10) or [Q]uit/[H]elp?
```

Image 1.1

Checking Caché/HealthShare Dataset Integrity

You can check the integrity of databases. This procedure is used to check the logical integrity of the Caché/HealthShare database on either a server or a client. Generally speaking, this procedure should be performed regularly (monthly or quarterly) on the server database and "as needed" on a local client database. "As needed" refers to a complaint by a clinician that their client is somehow misbehaving, or a routine client maintenance schedule implemented by the home health agency.

This procedure must be run by the NDoc system manager and presumes the system manager has a basic working knowledge of using the Caché/HealthShare System Management Portal.

Running the Check

To check the integrity of databases or globals stored in a database, do the following from the Home→Databases page of the System Management Portal:

1. Click Integrity Check to display a list of database names with check boxes.
2. Select the appropriate check boxes for the databases you want to check.
3. Click OK to begin the integrity check.

Warning: Do not run Integrity Check or the ^Integrity utility on a volatile database. Performing an Integrity Check while one or more processes are updating the database may result in the false reporting of database integrity errors.

Note: Enter the name and location of a log file. You can accept the default (integ.txt), click Browse to choose an existing file, or enter your own file name. The integrity check process runs in the background and saves the results to the file name in the text box.

Viewing Integrity Log

You can view the log resulting from the background process by:

1. From the Home→Databases page of the System Management Portal, click Integrity Log.
2. Enter the file name used in the Integrity Check process. The default named file displays if you used that name. Otherwise click View File to display your integrity log file.
3. You can search for strings within the log file. Enter the string and click Search. Matching strings are highlighted.

Note: Depending on the size of the databases this process may take a while. You can click 'View File' again to refresh the contents of the file on to the web page. It is recommended to give this process approximately 10 minutes to finish.

Analyzing the Results

Use the steps above in 'View Integrity Log' to view the integrity log first. Inside this window you can search for a particular string of text to highlight. When looking for possible errors the best thing to search for is 'Total for directory'. Once you have this text highlighted, scroll down through the file and look for the section shown below.

```
---Total for directory C:\ndoc\InterSystems\mgr\cacheaudit\---
        29 Pointer Level blocks         232kb (0% full)
        29 Data Level blocks            232kb (0% full)
         0 Big String blocks
        73 Total blocks                 584kb (0% full)
        55 Free blocks                  440kb
```

```
Elapsed time = 0.6 seconds 12:54:51
No Errors were found in this directory.
```

A section similar to the one shown above will display for each database. As long as you see the text 'No Errors were found in this directory', then the database is fine. The error messages can vary, but it is always recommended to take immediate action. If an error condition is encountered on a local client, it should be refreshed from the server (see Refreshing a Standalone/Local Client section for instructions).

Imaging or Renaming a Computer with Caché/HealthShare

Imaging a computer with NDoc installed is only recommended for the purpose of quickly rolling out a group of computers with NDoc. Any image created with NDoc installed runs the risk of causing the NDoc install to become unusable after a period of time without performing a refresh after the application of the image. This happens because the NDoc files in the image are not synchronizing with the server daily which causes it to go outside of file retention OR it can become outdated due to the Client Installer being updated. Refer to NDoc release notes or our website to find the latest version of installer (if you don't have access, ask the System Manager). The current version you are using is in the title of the installer file (i.e. NDocSetup_vx.x.x_x86 or x64). This could be avoided by creating an image every X amount of days, where X is less than or equal to the file retention setting on the server and will vary from client to client. Submit a request via the Thornberry Help Center for details on your server setup.

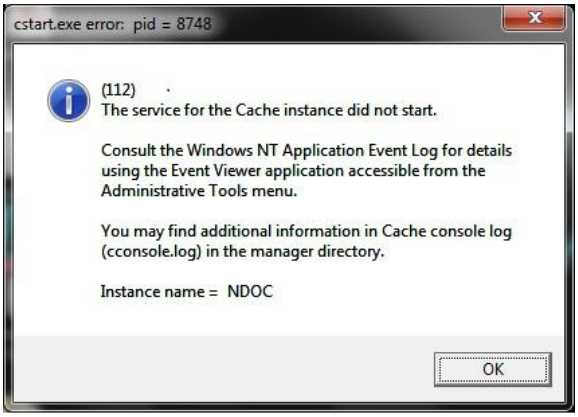
If you have a computer with either Caché or HealthShare installed and would like to rename the PC or image the drive, the cache.ids file must be deleted to allow Caché/HealthShare to startup properly. This file is created when Caché is installed and started. Without deleting this file, you see the issue detailed in *Troubleshooting* below. The steps to follow for imaging/renaming the PC are:

1. Install NDoc client (skip for renaming the PC) – DO NOT Refresh NDoc which is the final step of installing. Exit the Refresh screen and continue the steps below.
2. Shut down Caché via the Caché or HealthShare icon in system tray. (click and choose STOP)
3. Delete the cache.ids file from the \ndoc\Intersystems\mgr\ directory.
4. Create your image OR rename your PC.
5. Restart Caché via the gray cube (click and choose START) which recreates the cache.ids file. So for an imaging scenario this would happen on startup of the machine after the image is applied.
6. Refresh NDoc (skip for renaming the PC). Refer to the Refreshing a Standalone/Local Client section if you need instruction on how to do that process.

Troubleshooting issues with an Imaged/Renamed Local Client

Caché instance does not start

This error occurs if the Cache.ids file was not deleted during the making of your image or renaming your PC. This is because the cache.ids file is a machine specific file retaining the computer name. The cache.ids file can be found on the computer in the \ndoc\Intersystems\ mgr\ directory. Once you restart Caché/HealthShare, the file automatically is recreated with the new machine's name.



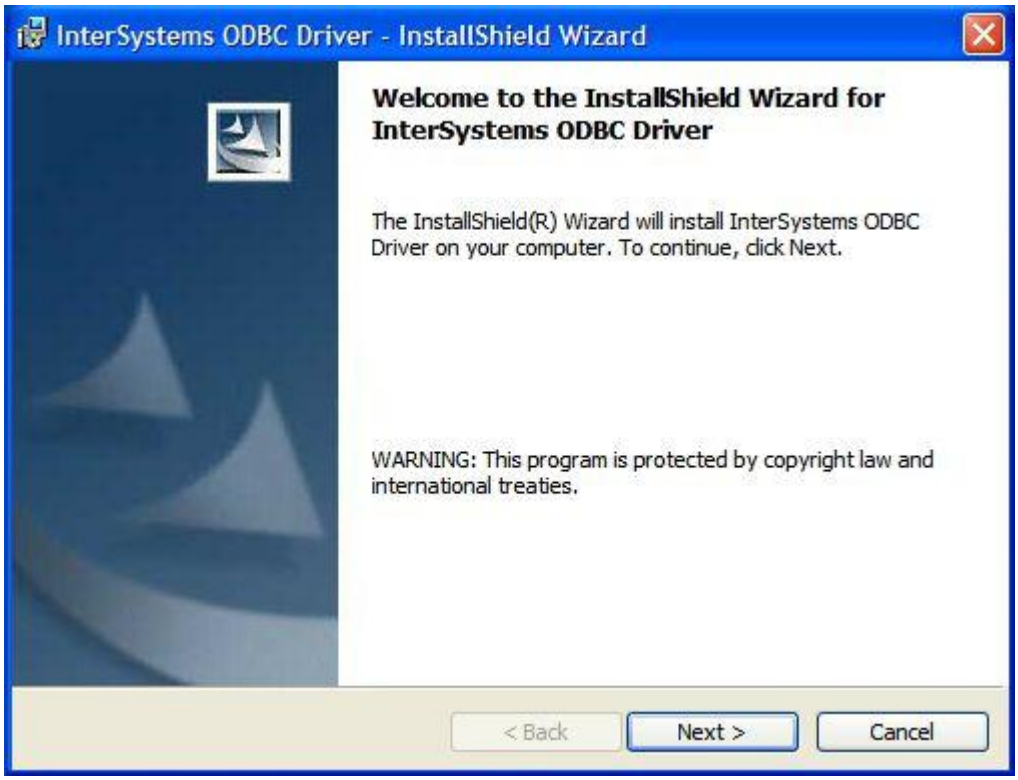
Configuring the Reporting Workstation (ODBC)

Setting up the client workstation that will run database access/reporting software (such as Crystal Reports, or Excel, Access, or other ODBC-compliant reporting tool) consists of loading the InterSystems Caché ODBC driver and setting up the NDoc ODBC Data Source.

ODBC Driver Installation

The InterSystems ODBC driver must be installed on each workstation licensed to run Crystal Reports. The ODBC driver can be downloaded from the client access portion of the Thornberry Ltd website. You must choose the driver that corresponds to the database installation you have currently, e.g. HealthShare 2014.1 ODBC driver is not supported to work against an HealthShare 2016.1 installation. Once the driver has been downloaded from the website follow these steps:

1. On the computer you are installing the driver for, extract the zip file you have downloaded to a location you can browse to.
2. Browse to the location the files were extracted to and run the executable file that is appropriate for your machine (e.g. x64 for 64-bit; x86 is most common).
3. Click Next, then Install to go through the install process.

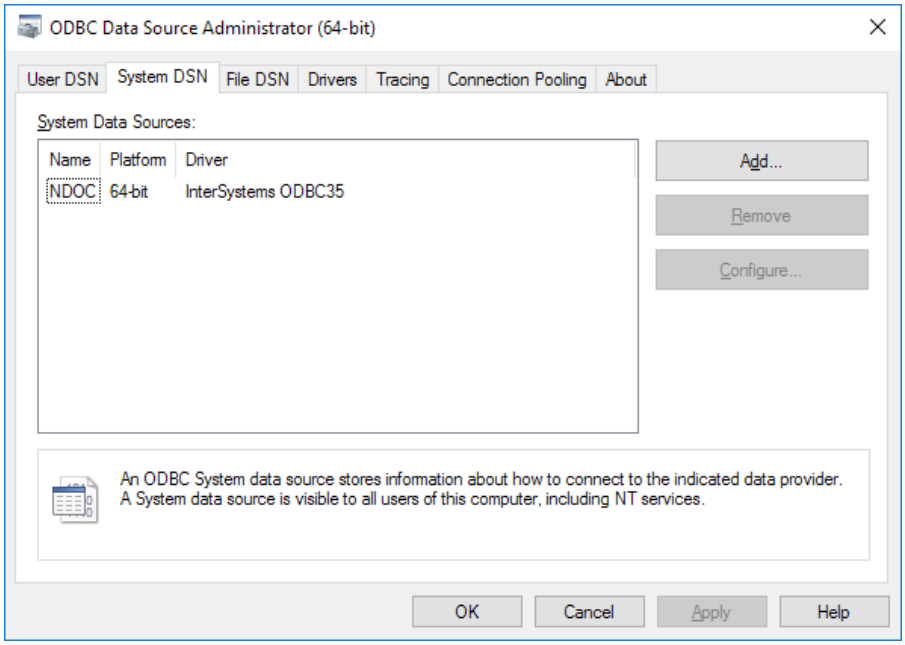


4. Click Finished, completing the install.

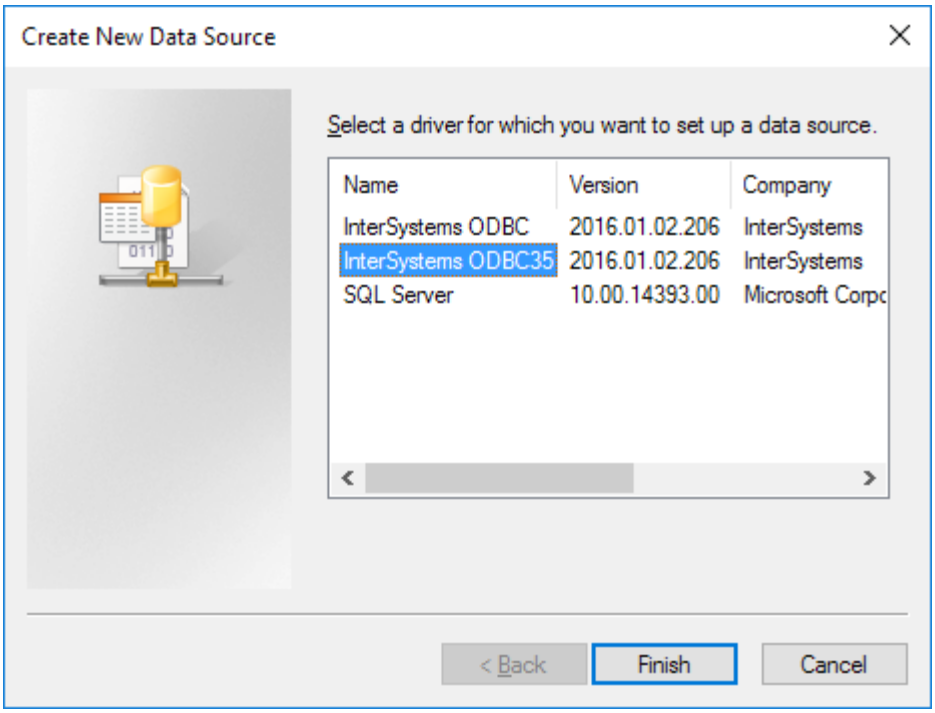
Configuration

An ODBC data source must be established that describes the location of the NDoc database and the driver used by ODBC to access the database. A data source named *NDoc* is built around the InterSystems' ODBC driver installed in the previous section.

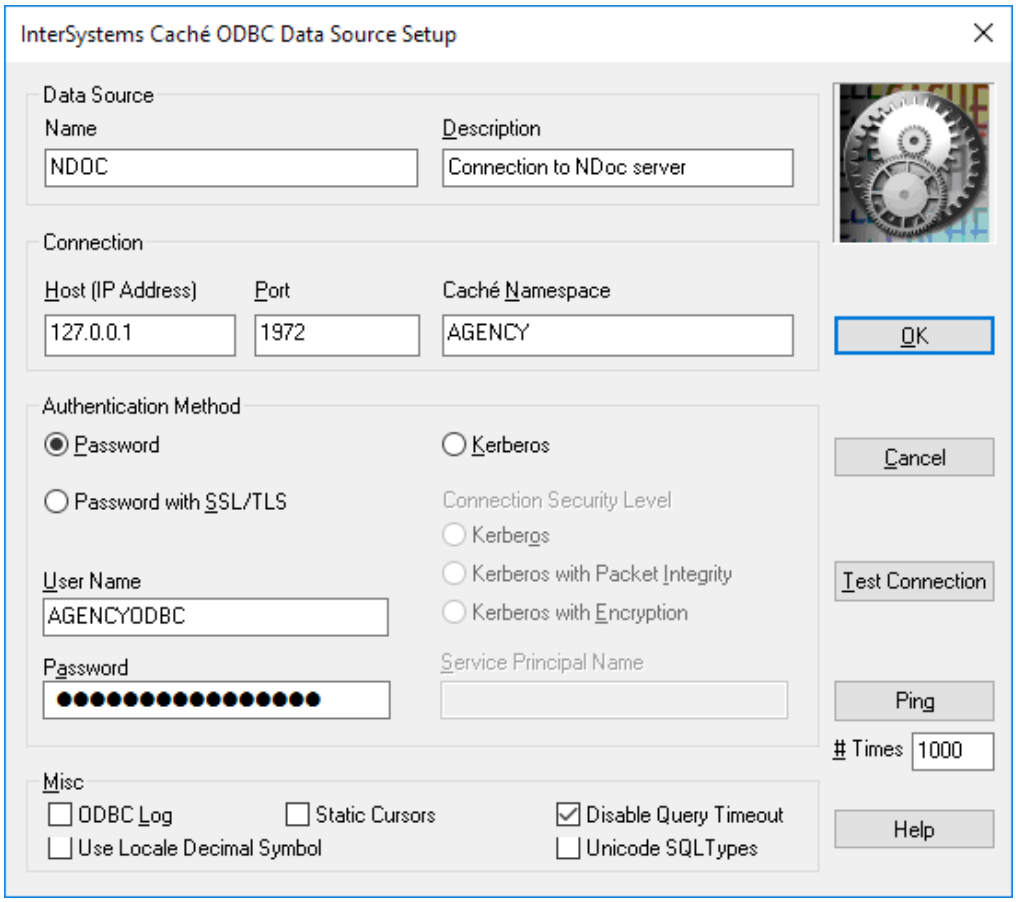
1. Navigate to Control Panel→Administrative Tools→Data Sources (ODBC). Open the Data Sources (ODBC) program.
2. Click on the System DSN tab. If you already have a DSN called NDoc setup then skip to step 5. **Note:** *NDoc appears in the image to the right because it has already been added as a System DSN. Once added, it will appear as shown, and the Configure function is used to modify its parameters.*
3. Click on the *Add* function.



4. Select the *Intersystems ODBC35* driver and click *Finish* (*see image to the right)*. If it is not available in your computer's ODBC driver list, try reinstalling the driver again first. If it still does not appear, contact Thornberry support



5. Configur*e the data sourc*e with settings specified be*low. The image* shown below will not *exactly* match your settings.
    a. **Data Source Name:** NDoc
    b. **Host (IP Address):** *Your NDoc server's internal IP address*
    c. **Port:** 1972
    d. **Caché Namespace:** *The name of your agency's namespace as specified by Thornberry.*
    e. **User Name:** *Supplied by Thornberry*
    f. **Password:** *Supplied by Thornberry*
    g. Check the **Disable Query Timeout** setting.



6. You should test your DSN configuration before saving and exiting the DSN configuration form by clicking the *Test Connection* button on the DSN configuration form. You should get the message '*Connectivity test completed successfully!*' if the settings are correct.

Standalone/Local Client Synchronization

This section discusses the theory and operation of the client synchronization process, a process extremely critical to the operation of NDoc. The synchronization process uploads charting from the local clients and downloads fresh patient charts. It is invoked from the NDoc Operations module by each field clinician on his/her client.

NDoc uses Secure File Transfer Protocol (SFTP) to synchronize clients to the server. The server creates files of patient data, agency table data and NDoc program updates to transfer to the clients. The clients create files containing patient data charted since the last synchronization. Both the server and clients communicate their status during the synchronization process by passing files between each device.

NDoc maintains these directories by deleting old files on based on file retention settings.

Automating Connections for Local Client Synchronization

In most cases the synchronizations for an NDoc client occur over the WAN, instead of the LAN. Due to this fact, NDoc has the ability to initiate a specific connection (e.g. Microsoft phonebook [Dial-Up, VPN], Cisco VPN, etc) that securely connects and disconnects to a network during the synchronization process. In order for this to happen, you will need to provide custom connection script(s) or utilize the set of scripts generated on the fly by NDoc. Here you will find instructions on creating and configuring a Microsoft phonebook connection that is compliant with the default connection scripts for NDoc and instructions on customizing the connection scripts to work with other connection names/types.

How it Works

There are two possible sets of connection scripts that can be called during the NDoc synchronization process. Each set of connection script files include a connect and disconnect script and are set up in the same manner. In the NDoc synchronization screen there are three sync options: Dial-Up, Broadband, and LAN. Depending on your NDoc settings, the Dial-Up and/or Broadband options may not be visible.

At the beginning of the synchronization process, NDoc will execute the connect script (from the connection script set) that corresponds to the option selected on the synchronization screen. The Dial-Up option will call the set including connect.vbs and unconect.vbs and the Broadband option will call the set including connectBroad.vbs and unconectBroad.vbs. The LAN option does not call any connection scripts. Once the synchronization process completes, NDoc will disconnect the connection using the relevant disconnect script (unconect.vbs or unconectBroad.vbs).

The connection files can be placed anywhere on the client machine, but the default (recommended) location is the %SYSTEMROOT% (Windows install) directory. To place the files in an alternative location contact the Help Center to configure this setting.

For information on installing a set of connection scripts with the NDoc client installer, please reference the NDoc Standalone (Local) Client Installation section in this manual.

Using the Default Connection Scripts

In order to use the default connection scripts that are generated automatically by NDoc, the connection must be a Microsoft phonebook connection configured with the options below in *Creating/Configuring an NDoc Compliant Microsoft Phonebook Connection*. The only other requirement for using the default connection scripts is the name of the connection. Name the connection **NDOC DIALUP** for the Dial-Up option and **NDOC BROADBAND** for the Broadband option.

Customizing Connection Scripts

The simplest way to accomplish this is to first login to NDoc on the client machine and attempt to connect using the connection type, Dial-Up or Broadband, you would like to configure/change to point to a different Microsoft phonebook entry. You can cancel this attempt as soon as the synchronization ends in a retry attempt or success. Now follow the steps below for the change (in bold) you would like to make.

Change to a different Microsoft phonebook connection

1. Navigate to the %SYSTEMROOT% directory or the location where the scripts are stored. Look for the appropriate connect script and open it in a text viewer, e.g. notepad.
2. Find the text (listed below) that corresponds to the connection type chosen and replace it with the name of the connection you intend to have it open and save the file.
    a. Dial-Up: `NDOC DIALUP`
    b. Broadband: `NDOC BROADBAND`
3. Perform steps 1 & 2 again using the related disconnect script file of the connection script set.

4. Test the connection by executing the connect and disconnect script files.

Change to another connection type

In order to change the script to use a different connection type, such as Cisco VPN client, the connection to be called must be able to be launched through a DOS prompt. Once you have the DOS command call working outside of NDoc from a DOS prompt, you can move on to the steps below.

1. Navigate to the %SYSTEMROOT% directory or the location where the scripts are stored. Look for the appropriate connect script and open it in a text viewer, e.g. notepad.
2. Find the text (listed below) that corresponds to the connection type chosen and replace it with the command line call to the connection you intend to have it open and save the file.
    a. Dial-Up: rasphone -d ""NDOC DIALUP""
    b. Broadband: rasphone -d ""NDOC BROADBAND""
3. Perform steps 1 & 2 again using the related disconnect script file of the connection script set and using the text below instead of the text in steps 2a-b.
    a. Dial-Up: rasphone -h ""NDOC DIALUP""
    b. Broadband: rasphone -h ""NDOC BROADBAND""
4. Test the connection by executing the connect and disconnect script files.

Note: For any command line call, the quotes must be doubled when it is placed in the *.vbs files. Notice the double quotes in steps 2a-b and 3a-b.

Creating/Configuring an NDoc Compliant Microsoft Phonebook Connection

To create a Microsoft phonebook connection compatible with NDoc, follow the steps below. You need to provide your specific connection (Dial-Up, VPN, etc) information, so make sure you have that available. The choice to use the default or to customize the connection scripts should be made prior to completing the steps below, because it will directly affect how the connection is named. If you choose to customize the connection script, you should make all those changes prior to completing the steps below; otherwise you will have to stop during the instructions listed to customize the script files. If you choose to use the default scripts, you should perform the connection option (Dial-Up or Broadband) within NDoc first, cancelling out after the first error that triggers a retry.

Windows 7

1. Open Network and Sharing Center (within Control Panel).
2. Click *Set up a new connection or network* (under *Change your networking settings*). This will start the New Connection Wizard window.
3. Click the Next button.
4. Select the option, *Connect to the network at my workplace* or *Set up a dial-up connection* that is appropriate for the connection type you want to create then click the Next button.
5. If you selected *Set up a dial-up connection* to step 4:
    a. Enter the phone number that should be dialed to make the connection.
    b. Enter the user name and password.
    c. Enter the name of the connection in the *Connection Name*. Note: The name you choose here is dependent on whether or not you want to use the default connection scripts within NDoc or if you would like to modify them.
    d. Check the option *Allow other people to use this connection*. Note: Not checking this option will cause the synchronization to be unable to find this connection (phone book entry not found error), without changing the service, Caché Controller for NDoc, to logon as the user that is currently logged in while creating this connection.
6. If you selected *Connect to the network at my workplace* to step 4:
    a. You may be prompted with *Do you want to use a connection that you already have?* Choose *No, create a new connection*. Click the Next button.
    b. Select the option relevant to your network setup on the next screen and click the Next button.

c. Enter the network address you will connect to for the VPN.
d. Enter the name of the connection in the *Destination Name* field. Note: The name you choose here is dependent on whether or not you want to use the default connection scripts within NDoc or if you would like to modify them.
e. Check the option *Allow other people to use this connection* then click the Next button. Note: Not checking this option will cause the synchronization to be unable to find this connection (phone book entry not found error), without changing the service, Caché Controller for NDoc, to logon as the user that is currently logged in while creating this connection.
f. Enter the user name and password (and domain if necessary).

7. Click the Create button and the connection window will appear. Close the connection window.
8. Test opening the connection by executing (double-clicking) the connection script file for the type of connection you are configuring; for Dial-Up use connect.vbs and for Broadband use connectBroad.vbs.
9. Test disconnecting the connection by executing (double-clicking) the disconnection script file for the type of connection you are configuring; for Dial-Up use unconect.vbs and for Broadband use unconectBroad.vbs.
10. If steps 8 or 9 did not work then examine your script file(s). Most errors exist due to typos in the connection name.
11. Run the file C:\NDoc\ utilities\connectTest.bat.
12. In the window that opens, enter the number next to the 'Launch/Configure' connection type you would like to configure. If the prerequisite is met, the option selected will launch the appropriate connection through the Caché database software.
13. A new 'Interactive Services Detection' window should appear (usually this is minimized in the taskbar) with the options to 'View Message' or 'Ask Later'. Click 'View Message'.
14. You will be redirected to another 'desktop' which will show the connection window for the connection specified in step 11.
15. In the connection window:
    a. Enter the appropriate username/password for the connection.
    b. Check *Save this user name and password for the following users* and toggle it to *Me Only*. Note: You can set this to *All users* if you would like. The downside is that it is less secure.
    c. Click Properties then click on the Options tab along the top.
    d. Uncheck the options:
        i. *Display progress while connecting*
        ii. *Prompt for name and password, certificate, etc*
        iii. *Redial if line is dropped*
    e. Change *Redial attempts* to '0'.
    f. Click the Ok button.
16. Click the Connect button to test the connection.
17. Click 'Return Now' on the 'Interactive Services Detection Window'.
18. Switch to the DOS command window, if it is not already the current window, and you should see the text '*Press any key to continue...*'. Press any key.
19. Since the connection you just configured should be currently connected, you will need to disconnect it using the menu you're returned back to. Enter the number for the disconnect option that applies to the connection you have just configured. Note: Since the connection was made under another user profile, you will not be able to disconnect the connection without using this menu.

Per-Diem Local Client Procedure

This describes the setup procedure for standalone/local clients that are to be shared by multiple clinicians. There are two methods described as well as a general setup needed.

General Setup for both situations

1. Create dummy User IDs such as per diem nurses User IDs using Administration > Employee > User ID Maintenance. EX: PERNURSE1
2. Whenever a new per diem nurse is added, you need to login as SYSMAN and sync the shared client so that the ID is sent down to it (all user IDs are moved to a client during a sync). It is assumed for either process that patients are assigned to the nurses within NDoc

Daily Procedure - client is assigned to the nurse

The advantage of assigning a client to the nurse is that patients assigned to that nurse have files created by nightly processing. These files then download to the client when the nurse logs in and does a sync. Everything can be controlled through the syncing process which will keep the client updated as well as download the nurse's patient files. The disadvantage is the fact that the System Manager must go in and reassign the client to the appropriate nurse the day before the nurse gets the client so the appropriate patient files get created for download.

1. The System Manager makes sure that any client that is given out is updated with the most current updates, table changes, login IDs by logging in as SYSMAN and syncing.
2. The System Manager assigns the client to the user using Administration>Employee>Assign Client Devices the day before the nurse is picking up the client so that patient files are created for download to the client.
3. When the nurse picks up the client:
    a. If in the morning for that same day - The nurse should login to the client and sync before leaving to retrieve all their patients for the day.
    b. If in the afternoon for the next day -Have the nurse do a sync overnight allowing the client to remain connected to receive the 4am sync. This uploads completed patient visit data to the server and with Nightly Processing downloads the patient files for the nurse.
4. If the client is going to a new nurse the next day, the System Manager reassigns the client to the new nurse the day before which again is the prompt for Nightly Processing to create the new nurses patient files which would be ready to download.
5. When the visit charting is done for that day, an evening sync is done once again to move the data to the server either by the nurse OR the System Manager logging in as SYSMAN depending on whether the nurse drops off the client to the agency or not. If the same nurse uses the client multiple days, they would continue to login and do the nightly sync to send data back to the server and download the latest patient files for the next day's visits.

Daily Procedure - client is not assigned to the nurse

The advantage of not assigning the client to the nurse is that the System Manager does not have to reassign the client to users. The disadvantage is that not only do syncs have to be done to keep the client updated, but that nurses must do the Receive Patients since files are not created for them during Nightly Processing. So there are extra steps for them.

1. The System Manager should make sure that any client that is given out is updated with the most current updates, table changes, login IDs, by logging in as SYSMAN and syncing.
2. When the nurse picks up the client:
    a. If in the morning for that same day - The nurse should login to the client after 6am and do a Receive Patients using patient Acct #'s before leaving to retrieve all their patients for the day.

b. If in the afternoon for the next day - Have the nurse login and do a SEND patient synchronization for each of the patients that were charted. Have the nurse login in the morning after 6am and do a Receive Patients using patient Acct #s before leaving to retrieve all their patients for the day.

3. When the visit charting is completed for that day, an evening sync is done once again to move the data to the server either by the Nurse OR the System Manager logging in as SYSMAN depending on whether the nurse drops off the client to the agency or not.

   If the same nurse uses the client multiple days, they would continue to login and do the nightly sync to send data back to the server. Then in the morning they would do a Receive Patients to download the latest patient information for that days visit.

   Note: Due to file retention on the local client, Nurse #2 could see Nurse #1's patients, because patients remain for a couple of days on the client.

Migration to Direct Connection Type

Standalone/Local Client

- Decide on network access method:
  - Air Cards, Smart Phone Tether, etc.
  - VPN Access or Direct:
- Test network access method in your area of operation
- Un-install the local NDoc client
- Perform the workstation setup
- NDoc licensing conversion if necessary

Migration to Terminal Sessions Connection Type

Standalone/Local Clients

- Decide on network access method:
  - Air Cards, Smart Phone Tether, etc.
  - VPN Access or Direct
- Test network access method in your area of operation
- Setup Terminal Server if one does not already exist
- Create active directory accounts for the users. Configure these accounts with the workstation setup
- Un-install the local NDoc client
- Create RDP shortcut on the local client
- NDoc licensing conversion if necessary

Tablet

- Decide on network access method:
  - Air Cards, Smart Phone Tether, etc
  - VPN Access or Direct
- Test network access method in your area of operation
- Setup Terminal Server if one does not already exist
- Create active directory accounts for the users. Configure these accounts with the workstation setup
- Choose and install a Remote Desktop Application
- NDoc licensing conversion if necessary

Medication Database Overview

The medication database embedded within NDoc is the National Drug Data File (NDDF), a creation of First Databank (FDB). NDDF is used by Thornberry under license from First Databank.

NDDF is one of the healthcare industry's most widely used sources of up-to-date drug information. It assists NDoc clinicians in creating and reconciling a complete patient medication profile, and in performing drug interaction and allergy screenings automatically and in real-time.

NDDF is embodied by a series of relational tables, updated by First Databank monthly, that comprises the NDoc medication database and are collectively the source for clinicians' medication profile entries and for drug-drug and drug-allergy interaction checking. Coding within the tables allows Thornberry developers to write NDoc program code that accurately assesses the relationships between entities and present appropriate alerts to clinicians during the course of using NDoc.

Critical to homecare clinician success is the integration of NDoc and NDDF and its timely updating. Caregivers need quick access to medication and interaction information, and need to know they are relying on a current medication knowledgebase when making clinical decisions and performing patient medication teaching.

Critical to NDoc system manager success are the seamless methods by which the database is loaded on a new NDoc local client and kept current with monthly releases of new/updated NDDF information. These methods involve the initial local client build/rebuild and the monthly NDoc update process. (The initial server install, including the then-current version of NDDF, is the purview of the Thornberry installation technician.)

Each month Thornberry receives a new version of the complete NDDF from First Databank, along with a new version of "incremental files" representing the difference from the prior month's complete NDDF. Both complete and incremental version files are loaded by Thornberry technicians onto Thornberry internal servers, which are then automatically incorporated into each regular monthly NDoc application update so they are available to customers via the following two methods.

NDoc Updates to the server

The NDoc application updates that customers install on their own servers, or that Thornberry installs on hosting servers, contain the latest NDDF "incremental files". Thornberry's update program code inserts the incremental changes into the medication database on the NDoc application server and forces the changes down to each local client with the rest of the monthly NDoc application update. No system manager intervention is required to keep medication databases up-to-date.

Continuity of Care Document ("CCD")

The Continuity of Care Document is a HITSP C32 V2.5 document that uses an industry-standard XML data format to transmit the status of a patient at the time of generation. This next-generation HL7 Version 3 document is typically passed from a discharging organization to an admitting organization, and contains relevant information on the patient's current state, such as Patient Identification, Race, Gender, Language, SSN, DOB, Phone, Contact and Next of Kin information, Medication List, Diagnoses, Problem List, Allergies, Lab Results, and Vital Signs. This then allows the receiving organization to provide smooth continuity of care, as important information is at hand in a standard format at the time of transfer.

CCDs are typically transmitted to a central HIE (Health Information Exchange) whenever key information is updated, via an industry standard secure protocol. HIEs receive such information from all healthcare providers in the geographical area and maintain a master database of this information.

Individual healthcare providers, when they contract with the HIE to become a participating vendor, can thereby become the immediate recipient of the latest version of the patient's CCD record whenever a transfer event, such as a hospitalization of a homecare patient, or a discharge of a patient from a hospital to homecare occurs. NDoc can both receive and generate CCD documents.

NDoc Licenses

Each employee accessing NDoc must be licensed as either an “authorized user”, a “casual user” or a “local client user”. A “key” installed on the Caché database server controls licensing for all three types of users. Thornberry generates and installs an initial key when NDoc is first installed, and creates subsequent new keys in response to customer purchase orders containing requests for new licenses. These new keys are emailed to the requestor who must use the following procedure to install each key within seven calendar days of its generation at Thornberry.

Keys can be temporary or permanent. When created from a customer purchase order, the key is temporary and expires 45 days from date of issue. Upon Thornberry’s receipt of payment for the new licenses, it issues a permanent key to the customer. If payment is not received within 45 days, NDoc automatically reverts back to the most recent permanent key.

License Definitions

Local Client Users: Any users currently assigned to a client in the NDoc Administration>Employee>Assign Client Devices function count toward your license limit. This does not include spare clients that do not synchronize to the server. Spare clients do not have a unique 4-digit number registered within the Administration>Employee>Assign Client Devices function. "Extra" clients (to accommodate infrequent or per diem client users) that have a unique 4-digit number in order to function within the NDoc environment must be licensed.

Authorized Users: we use the “named user” method to track and license LAN users (your office personnel), where each individual counts towards the license limit, not the number of workstations or concurrent users. The NDoc User ID Maintenance function allows you, the NDoc system manager, to designate a user as an authorized (licensed) LAN user. Any user not so declared remains the default “casual user”. The total number of users identified as authorized users cannot exceed the licensed “authorized user” count. The Caché database server will reject any attempts to access NDoc by users not identified as authorized LAN users, subject to the “casual user” count, below.

Casual Users: we use the expression "casual user" to describe employees or external resources, such as physicians, that are infrequent visitors to your Caché database server. Employees with infrequent access requirements could be a part time supervisor or a local client user that occasionally sits down to a workstation to browse to the server. Unlike office personnel, who are named users, the casual user count is concurrent. Each key is cut with 1 casual user license. When NDoc detects a user access attempt by a UserID that is not classified as “authorized”, the access attempt is rejected unless there is a free concurrent casual user slot available for the attempted session.

User ID Maintenance – Casual vs. Authorized Users

Each user by default is classified as “casual”. You should designate each office-based employee as “authorized” by changing the radio button on the User ID Maintenance page. NDoc will permit you to designate up to *x* number of employees as authorized users, where *x* is equal to your key’s Authorized User limit.

Assign Local Clients to Users – How NDoc Counts Clients

Each key permits a certain number of clients to be assigned to users and to connect to the NDoc server. If your agency is licensed for 50 clients, then up to 50 client/user relationships can be established in the “Assign Client Devices” function and up to 50 different clients can synchronize on a given day. Unassigned clients do not count towards the license limit when assigning users. An unassigned client can sync, but in so doing will reduce (by one, on that particular day only), the number of assigned clients that can sync before a license-exceeded condition occurs. NDoc will reject any client sync attempted by a user not identified as “owning” a standalone/local client (through “Assign Client Devices”), attempted by a client whose 4-digit number is not registered in the “Assign Client Devices” table, or attempted by either an assigned or unassigned client where the combined number of assigned and unassigned clients attempting syncs for that day already equals the license count. If any of these conditions is encountered, the user will see the message "<Laptop License Exceeded Condition In Effect>” on the Sync page.

Errors

This section outlines the more common issues that users may encounter during NDoc operation, along with corrective actions typically required.

Category: **Error**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Current Patient	If patient not in NDoc	No Match Found!	Recheck and Re-enter 3 letters in name, Patient ID number, Make sure the search parameter is appropriate to the patient type or that the search parameter is "off"
2	Visit charting	Attempting to chart in an already completed OASIS	Unable to chart this assessment - it has already been completed.	Assessment must be placed on hold before continuing. Check to see that you are in the correct visit and wish to continue.
3	An Open module	Attempting to close while Patient record still open	Cannot close this session in its current state.	A part of the patient record is still open. Go to the open record and close it, then close the module.
4	Visit charting	Entering regular time	Enter the time in military format (HHMM)	Enter time in correct format.
5	Visit charting	closing visit at the exact same time	You must enter valid start and stop times so that the visit duration is not zero	Change the start or stop time for the visit so the total time is > 0
6	Visit charting	Signing off visit	You must enter the required fields on THIS screen before you Sign-Off of the visit.	Review the "pink" fields and complete them in order to proceed.
7	Patient Calendar	When dragging a scheduled visit from one day to another.	Invalid rescheduling area. Please make sure the 'reschedule box' is green	Retry moving the visit until the header turns green, indicating a successful location to drop the visit.

Category: **Warning**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Visit charting	Attempting a visit out of frequency	Warning: This visit is not authorized. If the visit must be charted now, please take the appropriate follow-up action to ensure it becomes authorized.	Go to Physician Orders and enter appropriate frequency for the discipline.
2	Patient Calendar	When dragging a scheduled visit from one day to another.	The visual reschedule banner turns red if the area is not an appropriate area to drop the visit.	Drag the visit until the banner turns from red to green, then drop.
3	Care Pilot/Patient/ Disc Status	Attempting to discharge a patient with active Disciplines (Agency site setting)	Unable to discharge patient. Disciplines still active.	Discharge disciplines first then discharge patient.
4	Care Pilot (OPS)/Non-Skilled Care Plan	Attempting to create a care plan in the past	Warning: You are creating a care plan for more than 60 days ago.	Review time frame and add create dates to create a Non-Skilled Care Plan in the present episode.
5	Patient Calendar	Scheduling an employee who may not have time, has a conflict with her schedule, or is off	Warning: This clinician does not have time available for this visit the morning of {date}.	Click 'ok' then review the employee's availability. Reschedule visit to another employee that is available.

Category: **Reminders**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Care Pilot/Visit Charting	Closing out of a visit	NDoc Reminder: If appropriate for this visit, be sure to: 1. File OASIS as Complete, 2. Complete Notifications, 3. Update Patient/Discipline Status, Meds or Orders	If appropriate, follow these instructions to complete the necessary documentation.
2	Care Pilot/(OPS) Non-skilled Care Plan	Quitting the module before completing.	Before quitting, please Save or Cancel your current charting activity.	Click 'ok' and then either save or cancel your charting.
3	Care Pilot/(OPS) Non-skilled Care Plan	Attempting to chart a non-skilled care plan without a frequency for this discipline.	The discipline must have a frequency in the current or next cert period prior to creating a Care Plan.	Go to Physician Orders and enter appropriate frequency for the discipline, then return and enter the care plan.
4	Care Pilot/Visit Charting	When entering a visit within the 5 day window for a recert and the patient requires an OASIS.	Reminder: This visit falls within the 5-day OASIS recert window ending {date}. You might want to chart the recert with this visit.	The clinician can then decide to chart the OASIS Assessment on this visit.
5	485/Create 485	When creating a 485, a reminder tells you the actions required before creating the 485.	NDoc Reminder: Before creating a 485, be sure to: 1. Sign off of any open Visit for this patient; 2.Chart all Meds and Orders; 3. Refer all Disciplines; 4. Add Discipline Frequencies.	Click 'ok' and then complete any required documentation before proceeding.
6	Logging into NDoc	Once you have logged in, if your password will expire within the set # of days set in NDoc you get a reminder with the # of days left.	Please note: Your password will expire in {#} days.	At this point you can click 'ok' and continue or choose to go to password change and make the change.

Category: **Logic Conflict**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Visit Charting /OASIS	Attempting to document M2020 in conflict with Medication Compliance	Your selection for M2020 (Management of Oral Medications) conflicts with charting already done for Medication Regimen Compliance-Patient, specifically, the inclusion of 'independent: oral'. Please verify patient's independence with meds and make corrections to either field as necessary. (If M2020 should be '0' then be sure to check 'independent: oral' for Medication Regimen Compliance-Patient. If M2020 should be '1 or 2', then be sure to remove the checkmark next to 'independent: oral'.)	Review documentation in medication Regimen Compliance, and either correct this section or answer the OASIS question accordingly.
2	Visit Charting /Outcomes	Attempting to chart an outcome before completing the appropriate instruction/ intervention.	You must first chart "Instr: pain mgmt/symptom control pt method' in category 'Pain Mgmt' for 'Pain Problems' before charting this outcome. Please note that you may not resolve this outcome as long as the patient's comprehension of any related instruction is still charted as 'repeat instruction'.	Go back to the instruct section for Pain and review instructions; if appropriate change instruction to achieve or the response that states why it couldn't be achieved and then complete the outcome statement.
3	Visit Charting/ Outcomes	Attempting to chart a response that is inconsistent with prior charting.	M1302- Risk of Developing Pressure Ulcers cannot be 'No' when the Braden Scale score is 18 or less.	Return to Braden Scale to review results and determine the correct answer and then chart the appropriate response.

4	Visit Charting/ OASIS	Attempting to chart inconsistent information that will also go to the POC (485).	You are attempting to chart 'bowel/bladder incontinence' (Loc 18A-2) for Activity/Functional Limits, but neither M1610 [Urinary] nor M1620 [Bowel] indicate incontinence. Please verify status and make corrections to the appropriate fields as necessary.	Review documentation in Activity /Functional Limits, and either correct this section or answer the OASIS question accordingly.

Category **Confirmation**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Care Pilot/Calendar	Choosing an employee from a list	Select this employee?	You can either click 'ok' or if this is not the desired employee click 'cancel' and start search again.
2	Main Menu/Select Patient	In choosing a patient from the list	Select this Patient?	If this is the patient you are looking for, click 'ok', if not then click 'cancel' and choose the desired patient.
3	Closing a module	When quitting out of a module	Close {Module Name} session…. Are you sure?	If you still want to close the session then click 'ok' if not then click 'cancel'.
4	Admin/ Password Change	When changing your password, NDoc checked that the password meets password criteria.	Your new password has been accepted. To save your password, click SAVE.	Click "save" to save your password.

Category **Information**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Care Pilot/ Visit Charting/ Wounds	Information regarding choosing healed/closed as a status for the wound.	If photos have been added to this wound, you will no longer be able to change the status to "clear" the wound. If no photos have been saved, you will be able to change the status to something other than healed/closed on a subsequent visit, but doing so will clear all charting associated with the wound. If this wound is healed, please discontinue any wound care orders that pertain to this wound. Are you sure you would like to heal the wound?	If the wound is healed proceed to answering 'yes'; if the wound is not healed answer 'no'. If a photo is associated with this wound you are informed that you will not be able to clear the healed/closed status.
2	Confirmation of action	Completing an action and clicking on 'Save'	Saved	Click ok, no further action.
3	Care Pilot/ (OPS) /Non-Skilled Care Plan	When creating the aide care plan for the next cert period using the present care plan as template.	This care plan of {date}-{date} will be changed to {date}-{date}. If you want to add a NEW care plan, select 'Cancel' and then select 'Add New Care Plan'.	If the information is correct click 'ok' and 'save'. If you want to create a new care plan, select 'Cancel' and then select 'Add New Care Plan'.
4	Operations/ Intake	Entering a new patient, clicking 'save' NDoc checks against already entered patients.	No match found	Click 'ok' and continue to Register and Refer the patient.
5	Care Pilot/Visit Charting and in OPS/Intake Referral	When clicking on the required button for charting and no required items are found.	No required items found	Click 'ok' and continue on to quit from the visit.

Category **Drug/Drug and Drug/Allergy**				
#	**Locations**	**Action**	**Message**	**Corrective Action**
1	Drug/Drug	Entering a medication that has a known interaction with another medication already in Medication Profile.	Med #1\Med #2 Interaction Found, Severity Level, Mechanism of Action, Clinical Effects, Predisposing Factors, and Patient Management.	Depending on the severity level, the Clinician may contact the physician for further instructions on discontinuing this medication.
2	Drug/Allergy	Entering a medication that may be contraindicated due to patient allergy. Example of Patient allergic to Tetracycline being ordered Tetracycline.	Tetracycline contains Tetracycline Trihydrate which is an ingredient in the Specific Allergen Group Tetracyclines therefore tetracycline does pose a Specific Allergen Group level allergy risk to this patient.	The Clinician may contact the physician for further instructions on discontinuing this medication since the patient has an allergy to the medication.

Technical or operating errors may be encountered by your users:

Error Type/*Message*	**Corrective Action: Refer to Document**	**Corrective Action: Refer to Section**
Windows:		
Server access violation (reported by Caché to user)	Operations Manual	Windows Issues
Caché/HealthShare:		
Write to journal file failed	Operations Manual	Caché Console Messages
Diskfull	Operations Manual	Caché Console Messages
Diskhard	Operations Manual	Caché Console Messages
Database startup failure	Operations Manual	Preventing Caché Database Startup Failures/Troubleshooting a Caché Startup Failure
NDoc Local Client		
Server Error in Application "Default Web Site"	Operations Manual	Standalone/Local Client Installation, Troubleshooting section
Server Availability Error: Server is currently unavailable	Operations Manual	Standalone/Local Client Installation, Troubleshooting section
Dial-up synchronization will not work	Operations Manual	Standalone/Local Client Installation, Troubleshooting section
Synchronization starts but does not complete without error	Operations Manual	Standalone/Local Client Installation, Troubleshooting section
Invalid Client ID	Operations Manual	Refreshing a Local Client
Recover charting from a local client that cannot sync	Operations Manual	Recover Lost Charting

Auto-Email

Thornberry has created "automated email" functionality to provide an alert to designated email recipients (both customer recipients and Thornberry helpdesk personnel) when various incidents, such as the installation of an update, low disk space, etc., occur on the NDoc server.

Although the capability is installed by default on every customer server, the following steps must be taken by the agency's system manager and/or network administrator in order to utilize it:

1) An email address must be designated (either an existing one or a newly created one) which is able to send email through the local SMTP server. There is no need for this email address to be set up for RECEIVING mail unless your local system manager wants to be able to read failed transmission messages. Thornberry must be supplied the URL or IP for the email serve, the port and an email account name and password for this email address.

2) The agency may identify any number of local email recipients who will also receive automatic email messages from the NDoc server. We recommend, at least, the NDoc system administrator and an alternative contact in case the system manager is out of the office. Customers with cellular text messaging can be added to receive a text message of the alert to their phone.

Examples of "Auto-Email" alerts that are issued by NDoc servers:

Message Type	**Message Text**	**Action You Take**
Update installed	Update <<<curupdate>>> has been installed at <<<sitename>>>. Last known update installed was <<<prevupdate>>>.	None
Nightly processing incomplete	Nightly processing has encountered an error and is unable to complete.	Contact Thornberry after-hours support
Drivespace low		Contact Thornberry Help Center during normal business hours or after-hours support

NDoc Billing Installation

In order for billing users to access the NDoc Billing application, a local workstation client must first be installed. During the installation process, the client is connected via ODBC to the billing database that resides on the server. Once installed, NDoc Billing is executed by clicking the yellow Billing bar on the NDoc Start Menu.

Operating System Requirement:

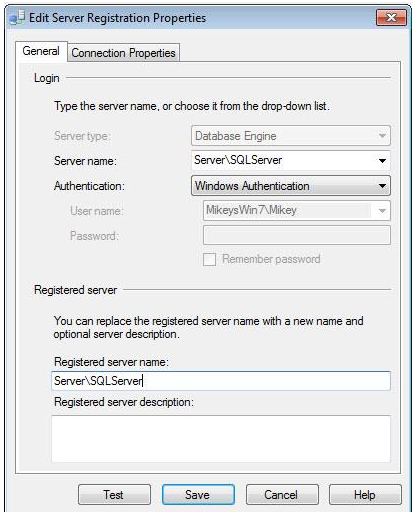
Active Directory/Domain Group – Active directory must be installed. NDoc Billing authenticates to the Domain. A Domain group should be setup called [Homecare] or something similar to identify the users who will be able to have access to the application.

Database Requirement:

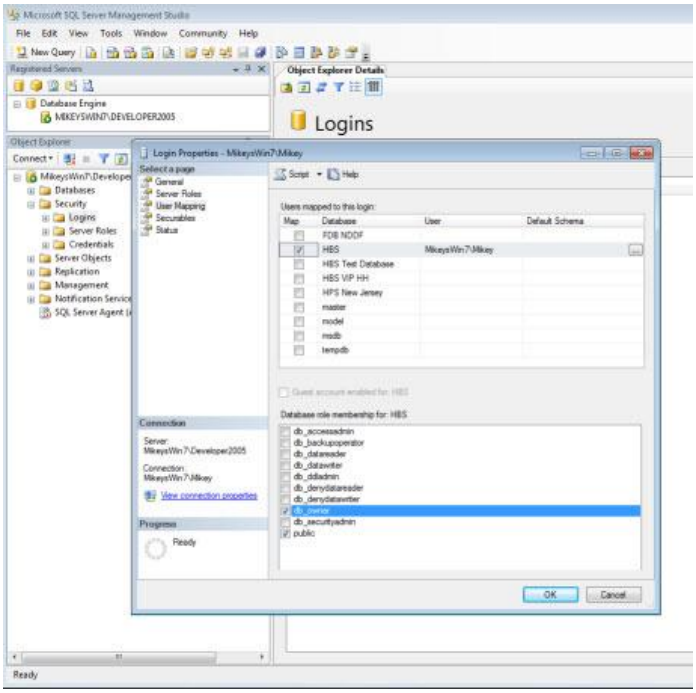
Microsoft SQL Server – Microsoft SQL server (2005, 2008 or 2008R2) must be installed. **Note:** The Express (free version) may suffice, but will start to slow down after 6-8 users are provided access, as it can only access 1 GB of memory and 1 GB processor.

Setup Options

- Windows Authentication should be specified during setup as seen below.



- **SQL Login** – An SQL Login must be created for the aforementioned group [Homecare], and allowed access as specified on the previous page. The login properties must allow access to all databases which the User (Group) will be accessing, and the User (Group) must have a DB_OWNER role as shown below.



Note – Please set up a regular SQL database backup per your internal disaster recovery policies.

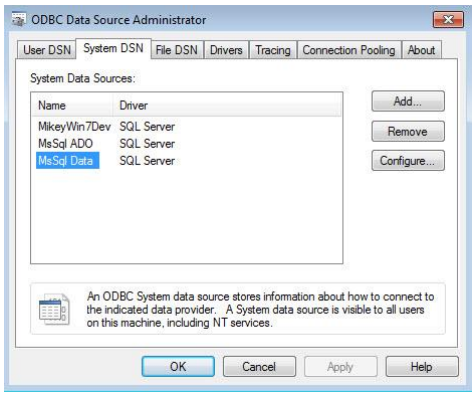
Server Access:

- **Access Type** – Access to the server must be available to enable the NDoc Billing installation team to load and authenticate the database and software. RDP is the preferred access method, but others can be used if RDP is not allowed. NOTE: Installation cannot proceed until the NDoc Billing team has access to the server.
- **Shared Folder –** The NDoc Billing team will setup a shared folder [\NDoc Billing] and 2 sub-folders within that folder called [\NDoc Billing Setup] and [\NDoc Billing Updates] on the server.
- **Installation File –** The NDoc Billing installation [Setup.exe] file will be placed in the \NDoc Billing Setup folder, and updates will be placed in the \NDoc Billing Updates folder. The client workstations will install the NDoc Billing system from the \NDoc Billing Setup directory, and get updates from the \NDoc Billing Updates directory, so they must be allowed "read" access to these areas.

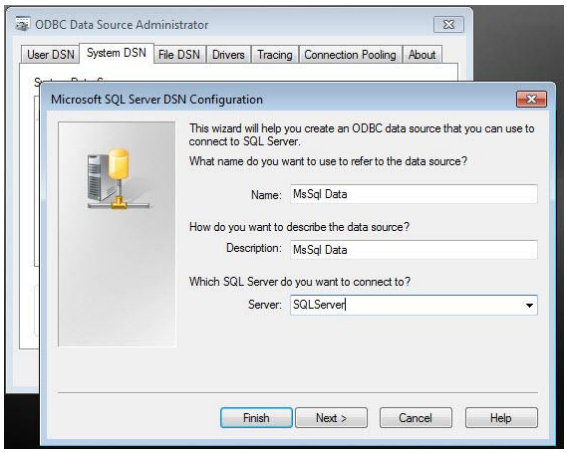
Workstation Setup:

- **ODBC data source –** Using the ODBC data source administrator, setup an ODBC source for SQL data which has the default database set to the NDoc Billing database as shown below.

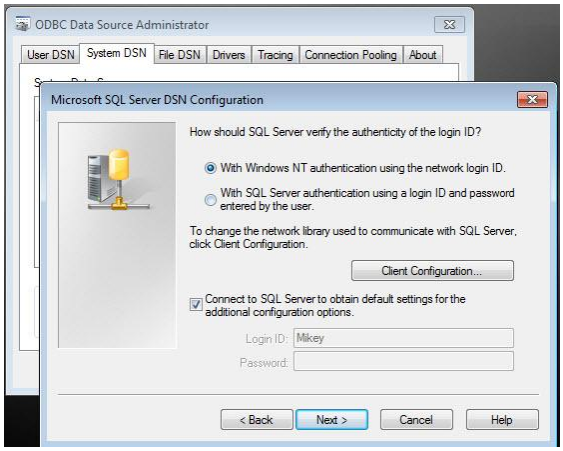
1. ODBC data source setup screen 1:



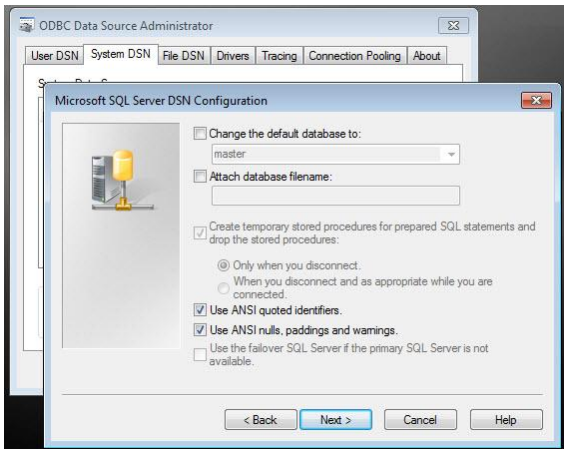
2. ODBC data source setup screen 2:



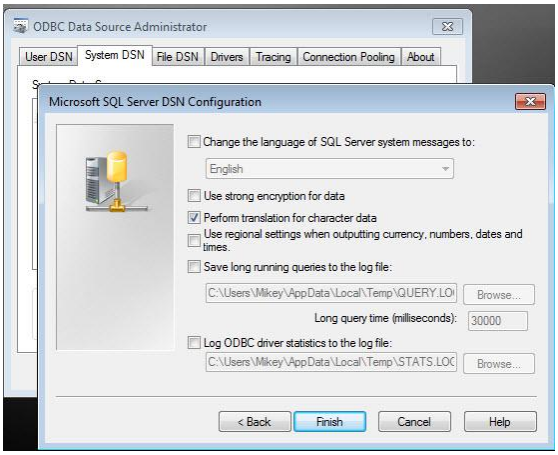
3. ODBC data source setup screen 3:



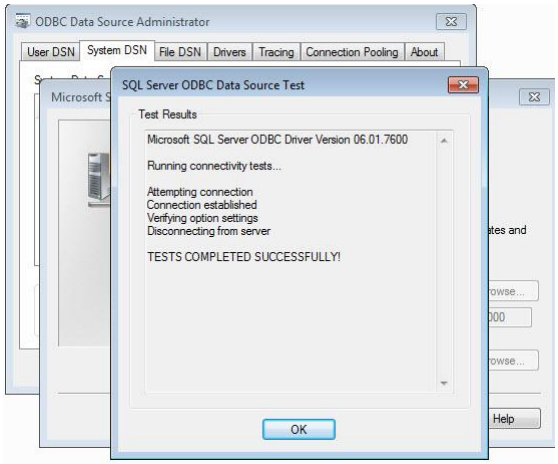
4. ODBC data source setup screen 4:



5. ODBC data source setup screen 5:



6. ODBC data source setup screen 6:

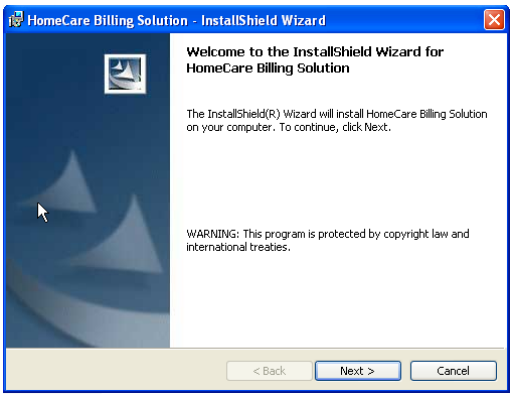


- **Data Source Test** – The previous step MUST give the message Tests Completed Successfully.

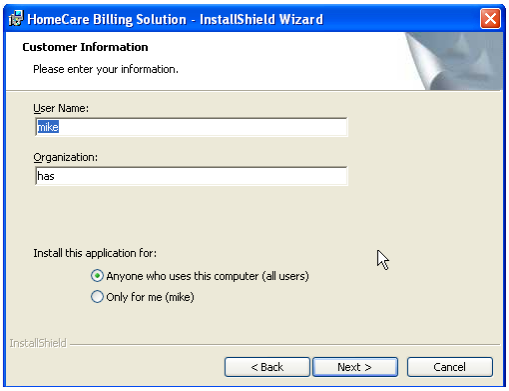
Client Installation

Installation – Install the NDoc Billing system by navigating to the C:\Billing Setup\ directory on the server and running the HBS_Setup.exe as shown below.

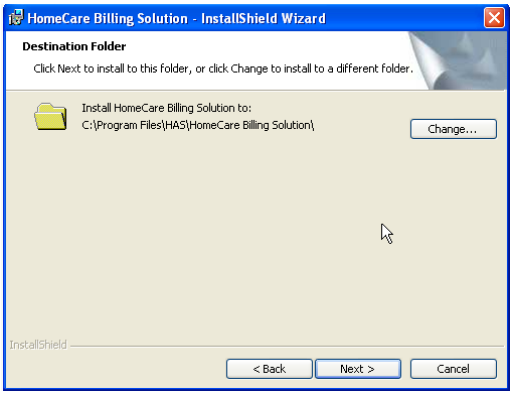
1. NDoc Billing Setup Screen 1:



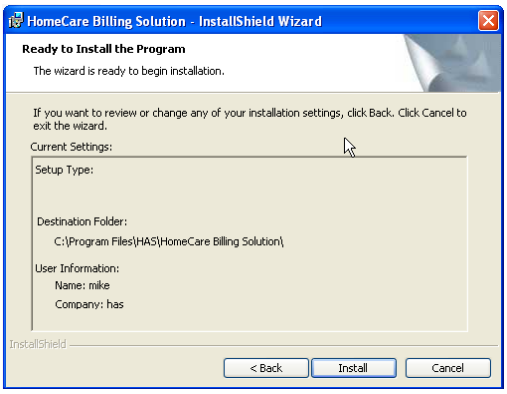
2. NDoc Billing Setup Screen 2:



3. NDoc Billing Setup Screen 3:



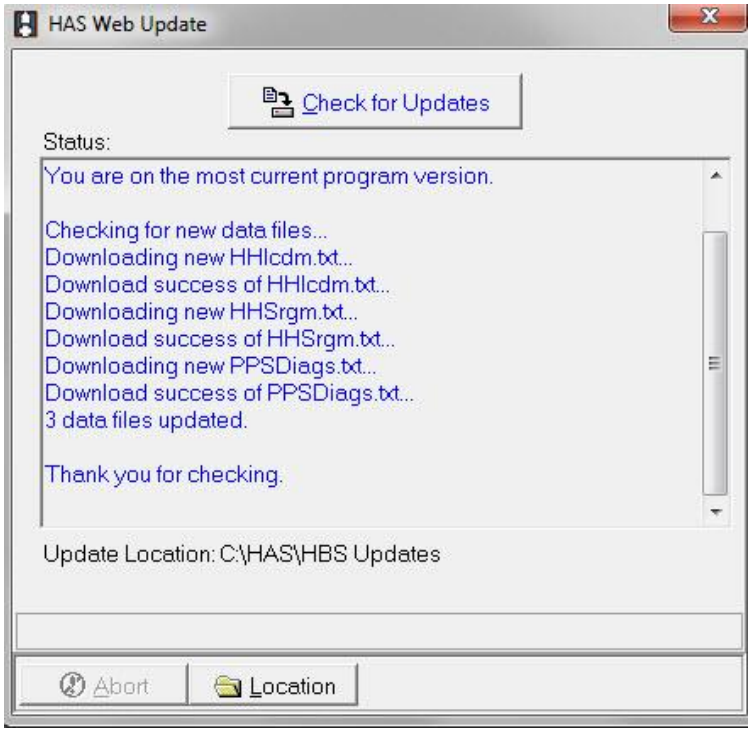
4. NDoc Billing Setup Screen 4:



NDoc (HBS/Netsmart) Billing - Web Updates

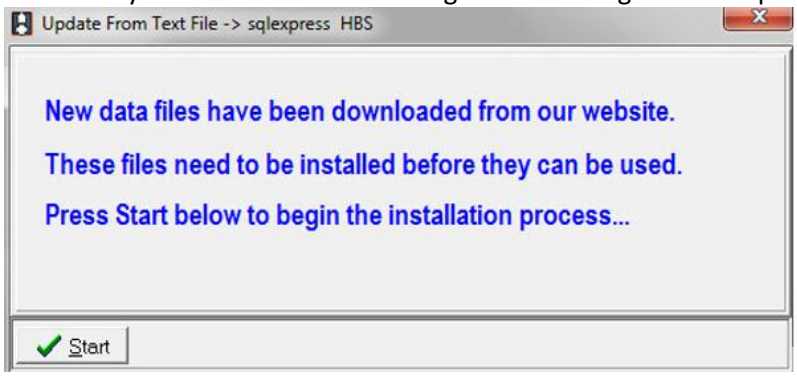
Description: This routine allows the user to download and/or install updates to the HAS software and data files. For "Check for Updates" to work, the following ports must be opened for inbound/outbound traffic to 100.26.123.241 on your firewall: TCP port 21 and TCP port 30000 - 65535. Additionally, some installations struggle to connect via TLS, which prevents the use of "Check for Updates". For installations struggling to use "Check for Updates", skip to the "NDoc Billing - Manual Updates" section below.

- On the server, click Help>Web Updates
- Enter the Master Password, when prompted, as defined in System Settings and then click the Check for Updates button.
- Note: If prompted to change your Update location, select the HBS Updates folder location on the server and open the HBSrun.exe file
- If there is no update available and you have the most current data files (ex. diagnosis or PPS Rates files) you will receive a message that you are on the current version and no update is needed. Otherwise updates will be downloaded:

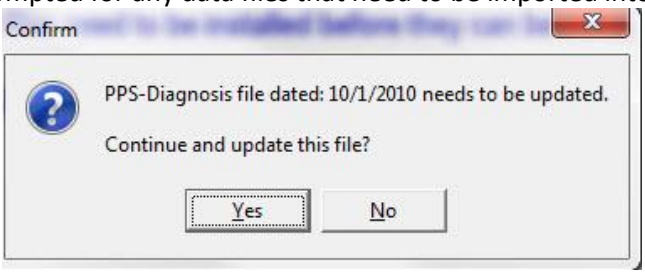


Data File Update

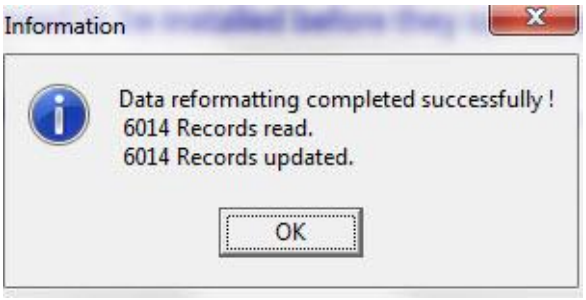
If new data files are downloaded you will receive this message when exiting the web update menu:



Click **Start** and you will be prompted for any data files that need to be imported into the current dataset:



Click **Yes** to import the data file.



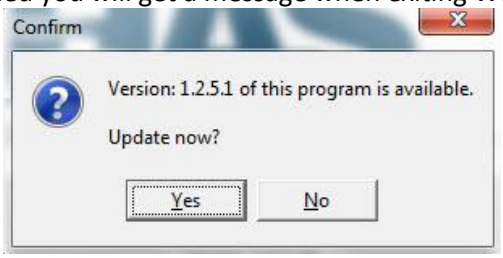
Program Update

Program updates are comprised of 2 steps:

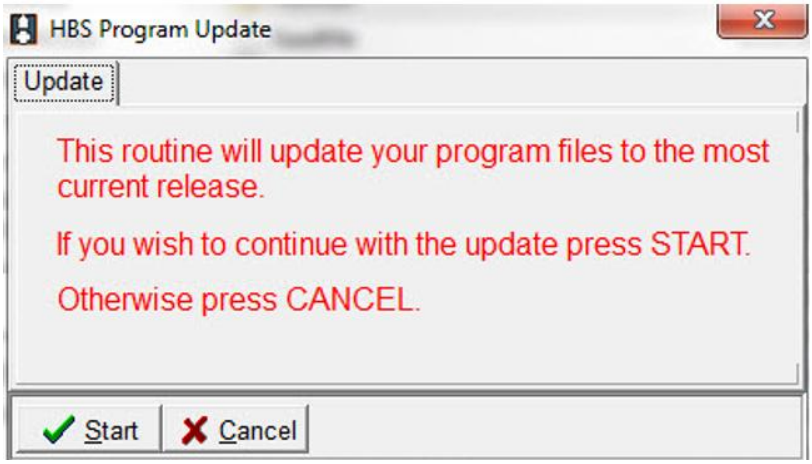
1 - Performing the Web Update to download the new program files to the agency's HBS Updates folder on the agency's server

2- Performing version updates on each PC to copy the newly downloaded program files from the HBS Updates folder to the user's local Program Files>HAS>Homecare Billing Solutions folder.

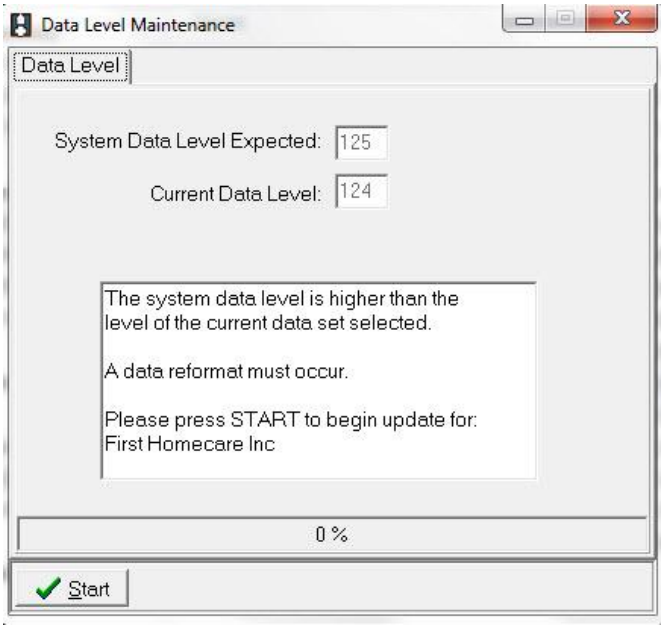
If a new program version downloaded you will get a message when exiting Web Update menu:



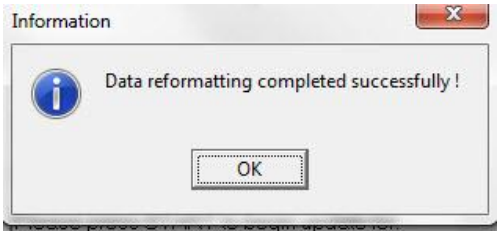
Select **Yes**, then click **Start**.



The program update may also contain a data reformat. If a data reformat is required you receive the following prompt:



Click **Start** to begin the data reformat. All other users should be out of the HBS program while the reformat is completed:



Note: The data reformat will need to done once for each company.

Each user will be prompted that the update is available the next time they go into NDoc Billing on their PC after the web update has been loaded.

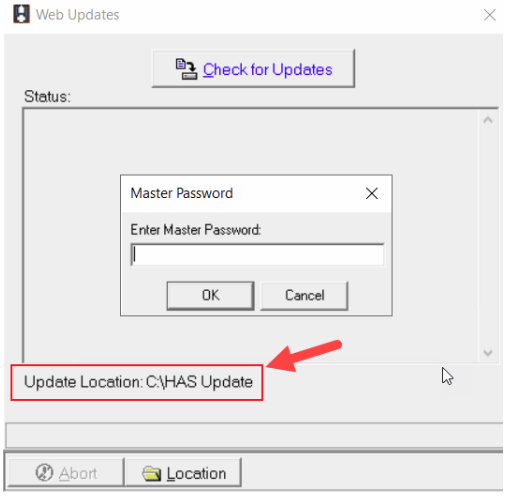
Note: In order to download the update from the web, a user would need web access and access to the Update Location on the server. To update their own PCs, users would need to be set up as local administrators or as power users with access to their own Program Files>HAS folder on their PC.

NDoc (HBS/Netsmart) Billing - Manual Updates

Description: This option allows agencies to manually download the program update from the NDoc Software website https://www.thornberryltd.com/ndoc-updates/ndoc-billing-updates. **NOTE**: This option is ONLY recommended to be used by agencies who are unable to use the "Check for Updates" functionality.

- Go the Thornberry customer Knowledgebase website under the NDoc Billing Update Files page.
- Download "NDocBilling_Update_{version}.zip" by clicking the button of the version **needed**.
- Copy the zip file to the server where "HBS Import/Export Service" is installed and running.
- Extract zip contents to the temporary directory.

- Copy contents of {temp directory}\HBS Update\ to the Update Location found in the Web Updates routine (e.g. {data drive}\HBS Update\) overwriting any duplicate files. Specifically, the files should be extracted to the same directory that appears in the bottom of the window when they open Web Updates in HBS.



  - ***NOTE**:* The exact directory will vary by agency settings
- Start NDoc (HBS/Netsmart) Billing, by using "Run As Administrator."
- NDoc (HBS/Netsmart) Billing will prompt you to update to the new version downloaded.
- After NDoc (HBS/Netsmart) Billing launches, go to Help→Web Updates, enter the master password, then close the dialog window
- When you close the Web Updates, you may be prompted to install data from the text files that are downloaded

Audit Trigger Events

These events in NDoc are recorded in our audit trail.

Trigger Point	Component	Event Type	Event	Notes
Caché Startup (SYSTEM^%ZSTART)	System	System	Start	
Caché Shutdown (SYSTEM^%ZSTOP)	System	System	Stop	
Caché Startup (SYSTEM^%ZSTART)	System	Security	Audit_Start	
Enable Auditing from Settings Page	System	Security	Audit_Start	
Caché Shutdown (SYSTEM^%ZSTOP)	System	Security	Audit_Stop	
Disable Auditing from Settings Page	System	Security	Audit_Stop	
NDoc Login	Application	Login	Login	
Refresh Login	Application	Login	Login	
NDoc Download Page Login	Application	Login	Login	
NDoc Logout	Application	Login	Logout	
NDoc Download Page Logout	Application	Login	Logout	
NDoc Timeout	Application	Login	Timeout	
NDoc Download Page Timeout	Application	Login	Timeout	
NDoc Session Terminate	Application	Login	Terminate	
NDoc User Lockout	Application	Security	User_Update	
Patient Registration	Application	Data	Patient_Create	
Patient Created by Interface	Interface	Data	Patient_Create	
Patient Summary	Application	Data	Patient_View	Patient Summary, Contact Summary
Select Patient	Application	Data	Patient_View	Patient search
Select Patient	Application	Data	Patient_View	Employee dashboard
Select Patient	Application	Data	Patient_View	Switchover patient
Select Patient	Application	Data	Patient_View	Tracking lab results
Select Patient	Application	Data	Patient_View	Patient Calendars
Select Patient	Application	Data	Patient_View	Visit Verification By Patient
Select Patient	Application	Data	Patient_View	Cancel Patient
Select Patient	Application	Data	Patient_View	Un-Cancel Patient
Select Patient	Application	Data	Patient_View	Batch modify scheduled visits
Select Patient	Application	Data	Patient_View	Visit approval
Select Patient	Application	Data	Patient_View	Assign unassigned visits
Select Patient	Application	Data	Patient_View	Order approval
Select Patient	Application	Data	Patient_View	Med approval
Select Patient	Application	Data	Patient_View	Assign Contacts to User
Select Patient	Application	Data	Patient_View	Assign Patients to User
Select Patient	Application	Data	Patient_View	Modify Charted visit
Select Patient	Application	Data	Patient_View	Non-NDoc Visit Entry
Exit visit charting w/ changes	Application	Data	Patient_Update	
Exit Non-Skilled Care Plan w/ changes	Application	Data	Patient_Update	

Trigger Point	Component	Event Type	Event	Notes
Exit Patient Activity w/ changes	Application	Data	Patient_Update	
Exit Patient Supplies w/ changes	Application	Data	Patient_Update	
Exit Patient Discipline/Status w/ changes	Application	Data	Patient_Update	
Exit OASIS Report Maint w/ changes	Application	Data	Patient_Update	
Exit Referral w/ changes	Application	Data	Patient_Update	
Exit back office visit entry w/ changes	Application	Data	Patient_Update	
Exit non-ndoc visit entry w/ changes	Application	Data	Patient_Update	
Exit batch supply entry w/ changes	Application	Data	Patient_Update	
Unfile patient referral	Application	Data	Patient_Update	
Cancel Patient	Application	Data	Patient_Update	
Un-Cancel Patient	Application	Data	Patient_Update	
Switchover patient	Application	Data	Patient_Update	
Modify Charted visit	Application	Data	Patient_Update	
Special edit	Application	Data	Patient_Update	
Exit patient profile w/ changes	Application	Data	Patient_Update	
Exit medications w/ changes	Application	Data	Patient_Update	Grid, medication approval
Exit orders w/ changes	Application	Data	Patient_Update	Grid, order approval
Exit allergies w/ changes	Application	Data	Patient_Update	
Exit document library w/ changes	Application	Data	Patient_Update	
Patient Updated by Interface	Interface	Data	Patient_Update	
Visit Updated by Interface	Application	Scheduling	Event_Create	
Patient Visit Scheduled	Application	Scheduling	Event_Create	Calendars, patient activity
Patient Visit Rescheduled	Application	Scheduling	Event_Update	Calendars, patient activity, batch modify scheduled visits, visit approval, modify charted visit, reassign visits, assign unassigned visits, contact activity
Patient Visit Cancelled	Application	Scheduling	Event_Delete	calendars, patient activity
Patient Search	Application	Data	Patient_Query	Patient & Contact
Order Added	Application	Data	Order_Create	Grid
Order Updated	Application	Data	Order_Update	Grid, order approval, tracking lab results
Medication Added	Application	Data	Med_Create	Grid
Medication Updated	Application	Data	Med_Update	Grid, medication approval
Local Client Synchronization	Application	Login	Node_Authenticate	
Visit Sign-Off	Application	Data	Signature_Create	
Med Reconcilation	Application	Data	Signature_Create	
485 Creation	Application	Data	Signature_Create	Automatic creation and Create 485 page
485 Review	Application	Data	Signature_Create	Final Approval (Signature for Printed Doc)
Order Completion	Application	Data	Signature_Create	"
Med Completion	Application	Data	Signature_Create	

Trigger Point	Component	Event Type	Event	Notes
Printing Reports	Application	Data	PHI_Export	All reports
Interface Exports Patient Data	Interface	Data	PHI_Export	
Interface Imported Patient Data	Interface	Data	PHI_Import	
NDoc User Created	Application	Security	User_Create	
NDoc User Changed	Application	Security	User_Update	
User assigned to local client	Application	Security	User_Update	
Patient Assigned to User	Application	Security	Patient_Assignment	
User Type Created	Application	Security	UserType_Create	
User Type Changed	Application	Security	UserType_Update	Log type that was changed
User Type Access Changed	Application	Security	UserType_Update	Log type that was changed
Document Type (User Settings)	Application	Security	UserType_Update	Log type(s) that were changed
Audit Settings Modified	Application	Security	Audit_Change	

180 Good Drive
Lancaster, PA 17603

888-797-NDOC (6362)

www.thornberryltd.com