NDoc Software

Thornberry Hosted Services Manual

The information in this guide has been carefully checked and is believed to be accurate. Thornberry assumes no responsibility for any inaccuracies, errors, or omissions.

Thornberry reserves the right to revise this publication and to change its content without obligation to notify any person of the revision or changes.

Table of Contents

Overview

For customers who have chosen to avail themselves of Thornberry's Hosted Services; functionality and use of the NDoc application itself is generally equivalent to the experience of non-hosted customers. However, there are some notable differences in method of access, management of field devices, and maintenance of the server environment that users should be aware of. This manual seeks to clarify each area of difference in order to ensure clarity of implementation and setup.

Connecting to NDoc within the Hosted Environment

Access to NDoc and HBS Billing (when applicable) is accomplished using a single service. The following instructions detail the process for accessing applications provided within Thornberry's Hosted Services.

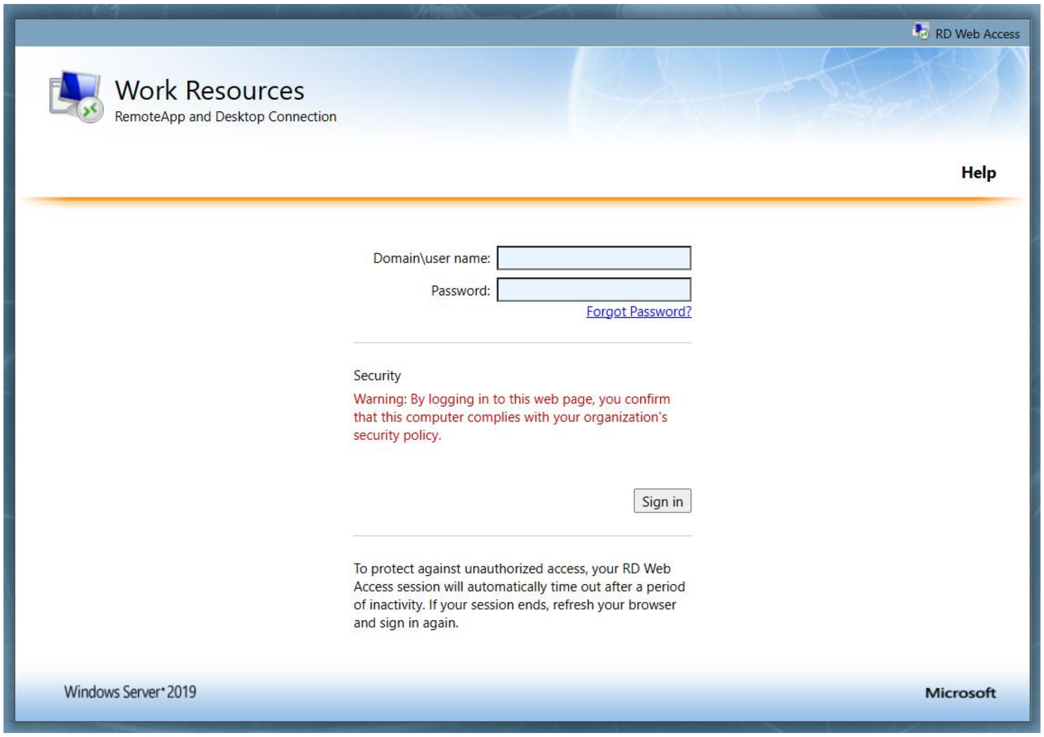
Configuring Multi-Factor Authentication for MyApps Access

In an effort to further enhance security protocols and protect data, Thornberry requires users accessing the hosted server environment to set up multi-factor authentication (MFA).   When new users are initially issued their MyApps username and temporary password from the Thornberry Hosted Solution Support Team, they should complete the steps to verify their MyApps credentials and confirm their updated unique password BEFORE taking the steps to configure MFA as outlined in the NDoc Reference for Setting up Multi Factor Authentication (MFA). The MFA prompt to approve the sign in to the hosted site is described below.

Connecting Using MyApps Connection

Open Google Chrome or Microsoft Edge browser and go to https://myapps.ndoc.net/

When prompted, enter the Domain\username (i.e., **NDOC\myusername**), using the username for remote desktop as provided by Thornberry Ltd. In the password field, enter your password for remote desktop as initially provided by Thornberry Ltd or from the Change Your Password routine. Click **Sign In**. NOTE: this password will be different from the NDoc password.

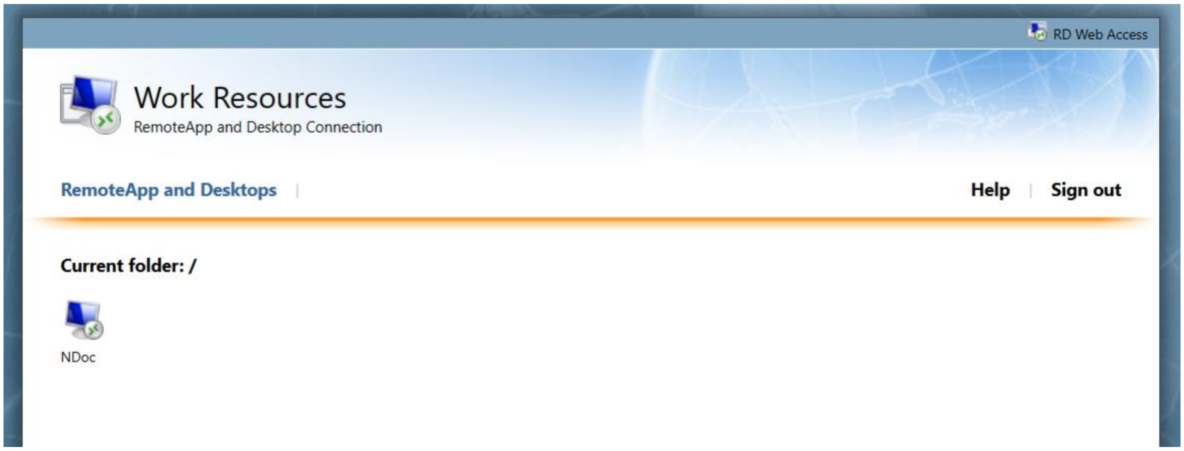


Security

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

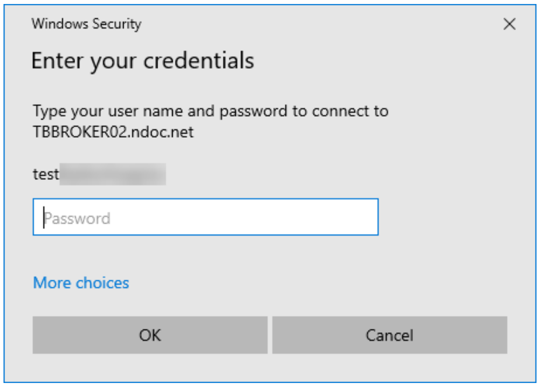
To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

You will land on the main page to launch the NDoc Desktop Application. Click the **NDoc Desktop Icon** to open and access desktop functions.



Current folder: /

Depending on the browser, users will see a prompt to download/open the RemoteApps file. When the download occurs, users are again prompted with a security pop-up to again enter their credentials:



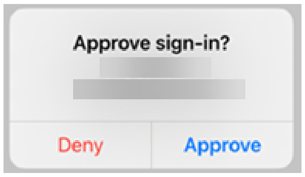
Enter your credentials

Type your user name and password to connect to TBBROKER02.ndoc.net

test[redacted]

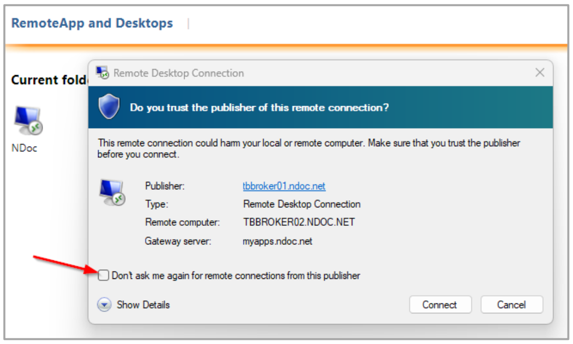
Password

With MFA in place, the Microsoft Authenticator will send a push notification to the user's phone. With that notification, users will be asked if they want to Approve Sign In. Clicking Approve will allow your MyApps login process to move forward.


Approve sign-in?

[redacted]

When prompted with the message related to trusting the publisher of the remote connection, check the box for "Don't ask me again for connections to this publisher," then click the Connect button.



Do you trust the publisher of this remote connection?

This remote connection could harm your local or remote computer. Make sure that you trust the publisher before you connect.

Publisher: tbbroker01.ndoc.net

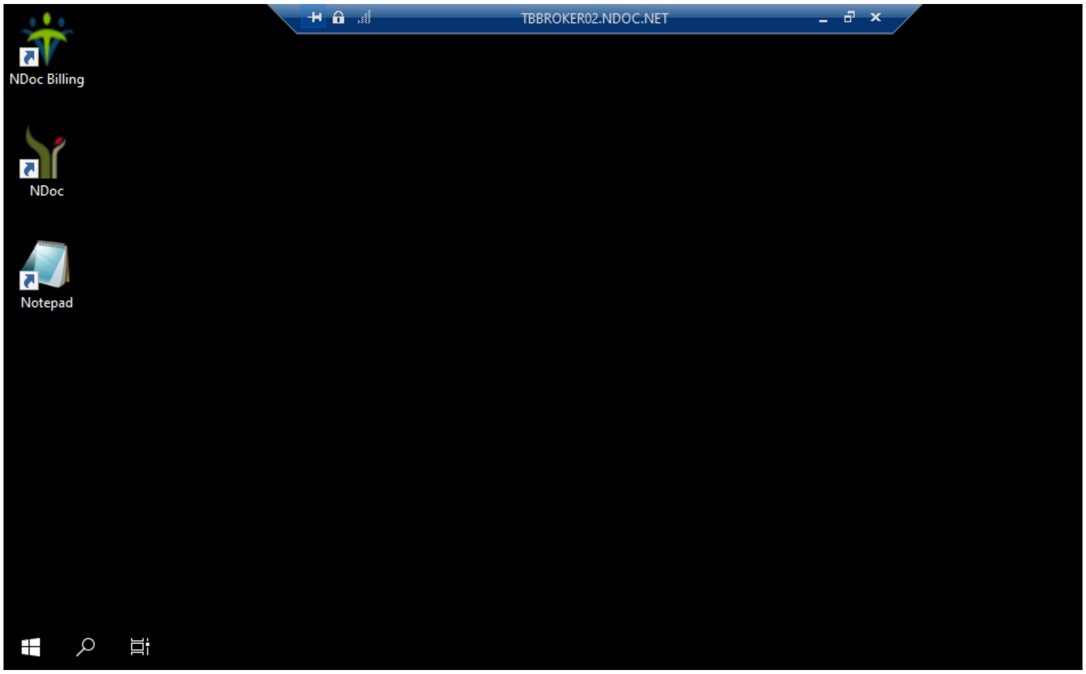
Type: Remote Desktop Connection

Remote computer: TBBROKER02.NDOC.NET

Gateway server: myapps.ndoc.net

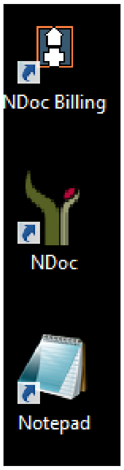
□ Don't ask me again for remote connections from this publisher

After the remote desktop session loads, a Windows desktop displays (*see image below*).



Opening NDoc and NDoc Billing

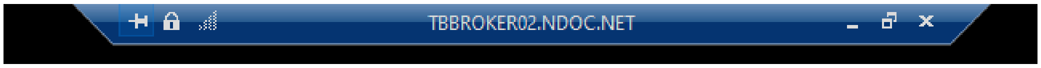
Once you have logged into your remote desktop session you can access NDoc and NDoc Billing by clicking the appropriate icons found on your desktop.



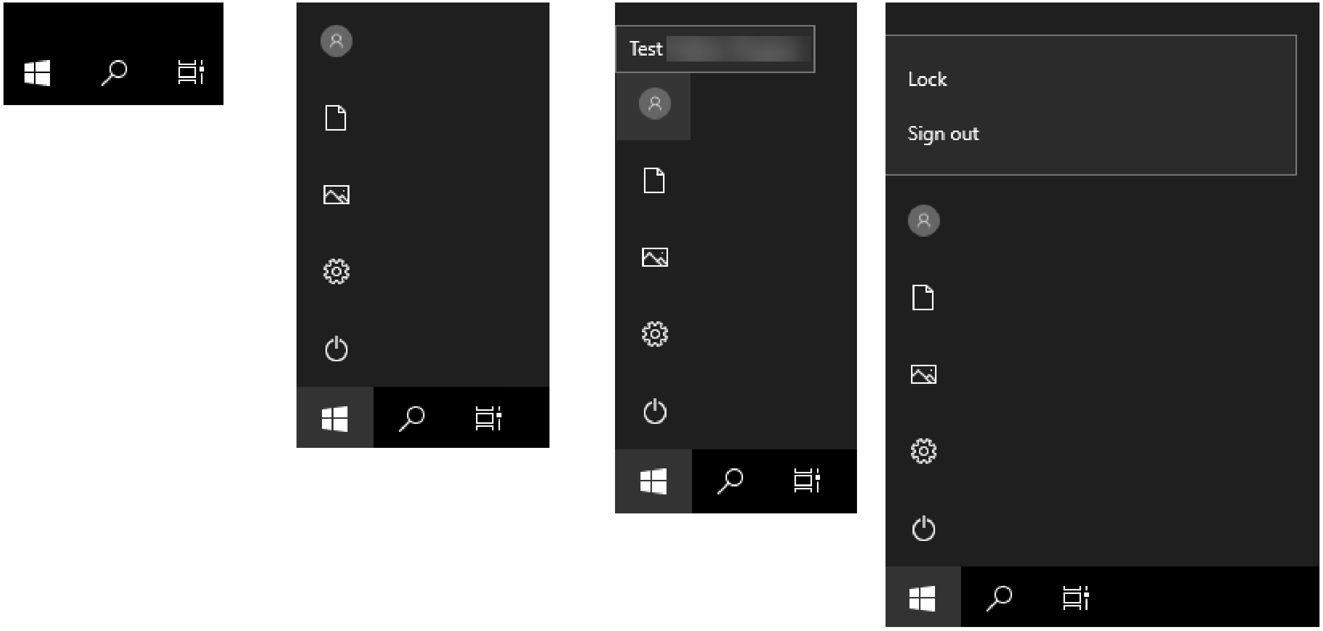
Remote Desktop Logoff Procedure and Reconnection

There are multiple ways to exit a remote desktop session; one will cause the session to remain open for a period of time on the server so that you can reconnect to it and the other will perform a normal Windows log off procedure for the session, making the session no longer available for reconnection. The primary difference between these two types is the ability to reconnect to the session.

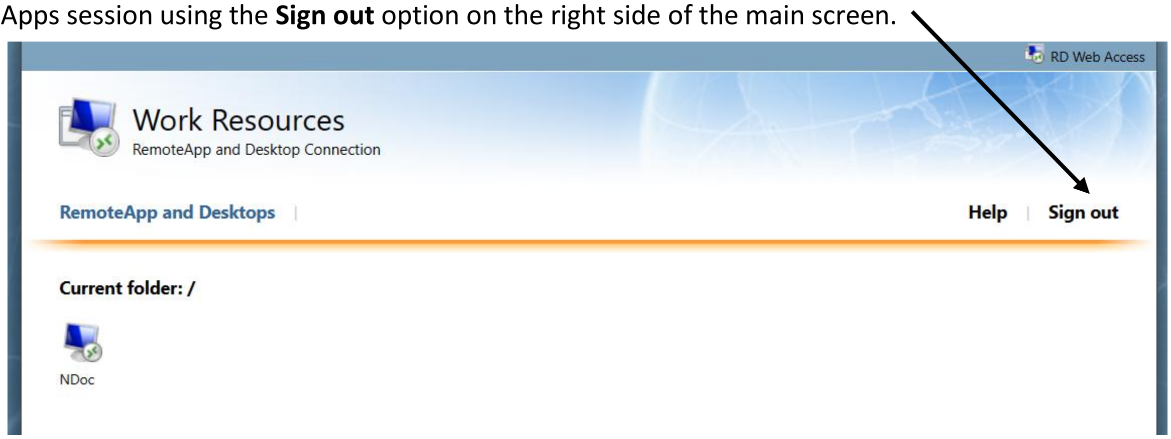
The first method can be accomplished by hovering with the mouse pointer at the top-center of the screen until a dropdown appears. The dropdown contains the normal Windows buttons for minimize, maximize/restore, and close. Clicking the **X** button will *disconnect* your session.



Another way to exit a remote desktop session is to click the **Start Menu** button (Windows icon) in the bottom left corner and open the menu to see the User icon. Hovertext will appear to identify the user. Click the icon and then click **Sign out**. This will close the session on the server completely

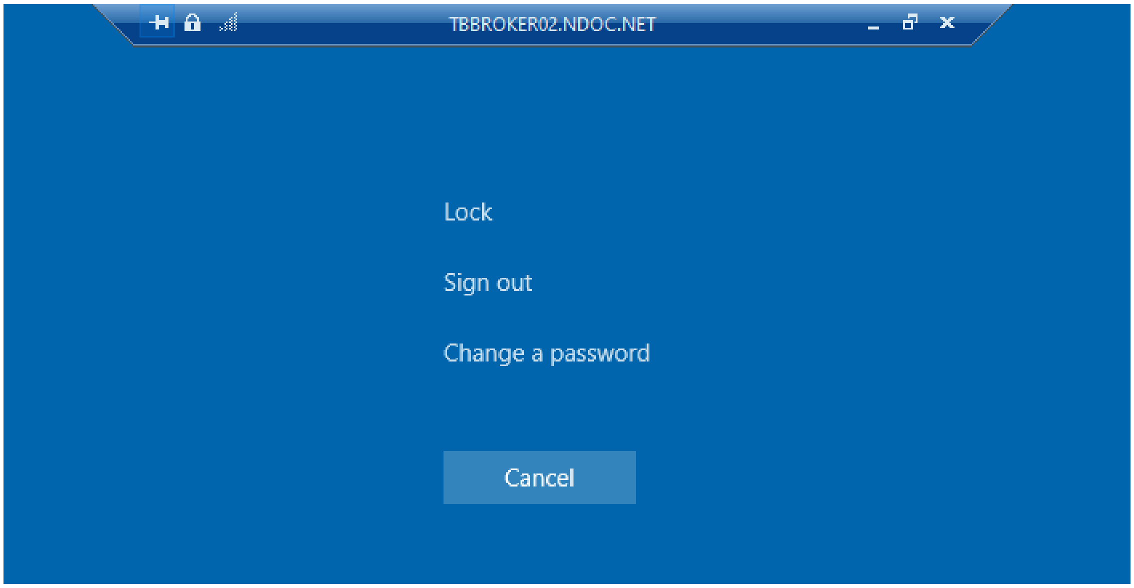


In addition to the process of signing out of the remote session, users must also take the step of signing out of the MyApps session using the **Sign out** option on the right side of the main screen.



Changing the Remote Desktop Password from the Desktop

1. While logged into Remote Desktop, perform the key combination **Ctrl+Alt+End**. ***Hint***: *Think of this the same way you would Ctrl+Alt+Del*
2. Once the screen changes, click the option "**Change a Password….**"



3. When prompted enter the old password in the first box. Then enter the new password in the next two boxes and hit **Submit**. You will see a message indicating your password has been successfully changed. Click OK

Terminal Session Handling

Disconnected Session Reset	2 hours	The elapsed time before a session is reset and no longer exists, after disconnecting from a session without logging off.
Active Session Limit	1 day	The elapsed time since the session initially began.
Idle Session Limit	2 hours	Session is still connected from the user's location but is sitting idle with no activity.

NOTE: The Idle Time and Disconnected Session timing is sequential. When the Idle Session Limit is hit, the session becomes a Disconnected Session. Additionally, just "X"-ing out of the RDP session would make the session become a Disconnected Session. Another 2 hour timer would start for the Disconnected Session before the session is Ended and the user is logged off.

Password Policies

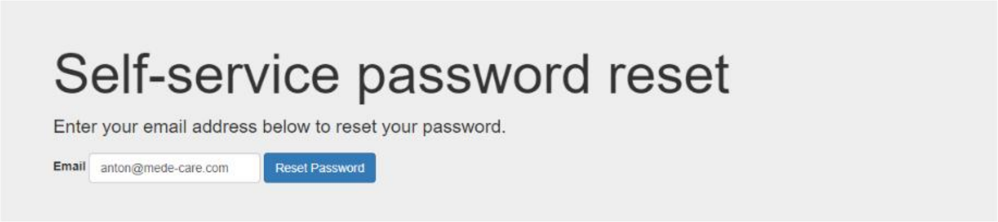
Expiration	90 days
Minimum Password Age	Users can only change their passwords 1x a day themselves
Complexity Requirements	Cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters Contains characters from three of the following four categories: English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, $, #, %)
Length	14 character minimum
Account lockout duration	Will be automatically reset after 60 minutes
Account lockout threshold	6 invalid logon attempts
Password History	Users cannot reuse a password from the last 3 passwords

If for any reason a password needs to be reset, please review the "Forgotten Password/Locked Account" section of this manual for instruction. Should use of that functionality prove ineffective, an authorized Help Center user should submit a request directly to the Thornberry Help Center. The support team will reset the password with a unique value and notify the requester accordingly.

Forgotten Password/Locked Account

If you have forgotten your password or you are being prevented from logging in due to multiple unsuccessful attempts, click the "Forgot Password?" link displaying beneath the Domain/Username and Password prompts on the MyApps login screen. **Note – In order for the next steps to be successful, customer must have already provided Thornberry with an email address for the relevant user.**

1. Click the "Forgot Password?" link to launch the prompt below. Customer should enter their registered email address in the available "Email" field and click "Reset Password."

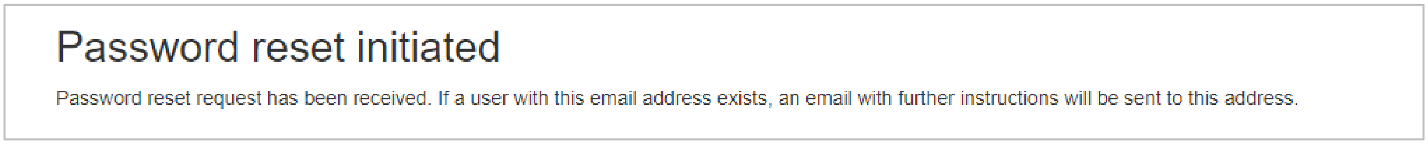


Self-service password reset

Enter your email address below to reset your password.

Email: anton@mede-care.com

2. After clicking “Reset Password,” the “Password reset initiated” message (below) will display to alert the user to watch for an email to their registered email address.



Password reset initiated

Password reset request has been received. If a user with this email address exists, an email with further instructions will be sent to this address.

3. After receiving the “Password reset initiated” messaging, if an email is associated with the user, they will receive an email from bot@thornberryltd.com at their registered email address indicating:

   “Your new temporary password is:

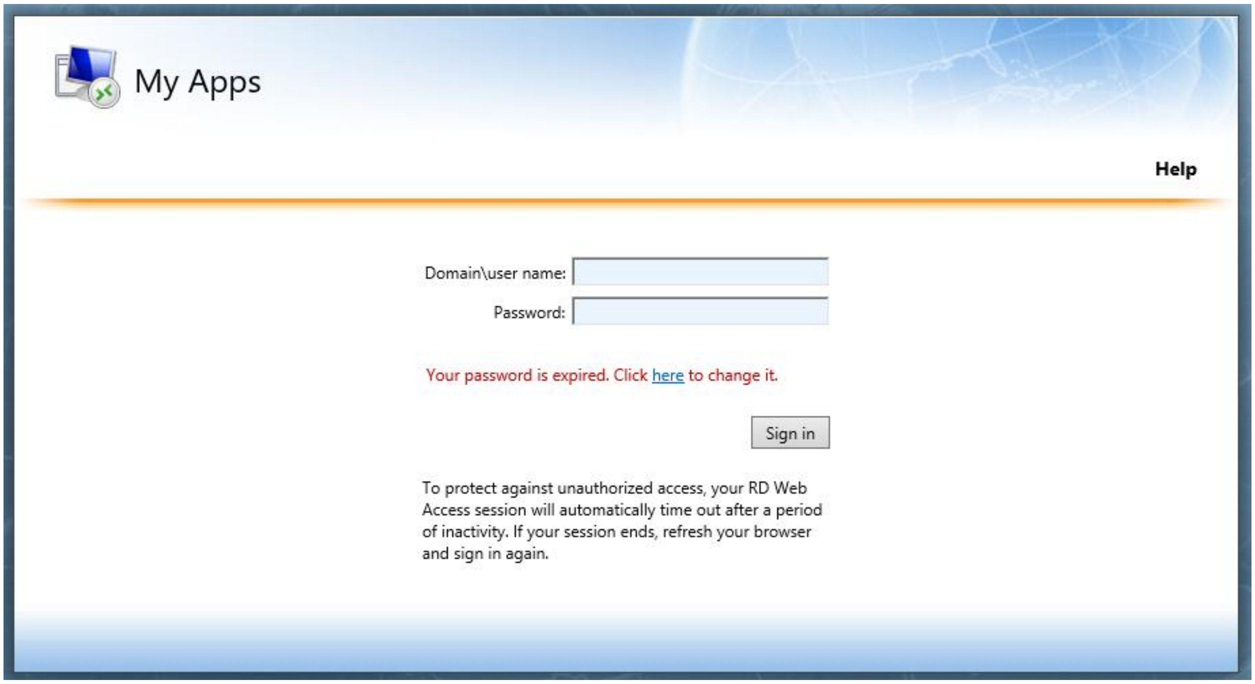
   [new temporary password]

   You will be asked to change the password the next time you log in to the system.”

4. Once a temporary password is received, the user should follow their typical MyApps login procedure, entering the received temporary password when doing so, and then using it again as the “old password” when prompted to set their new password.

Password Expiration

If your password has expired, you should see a message indicating the account has expired. Follow the prompts on the screen to make the change using the same logic as described above.



Your password is expired. Click here to change it.

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

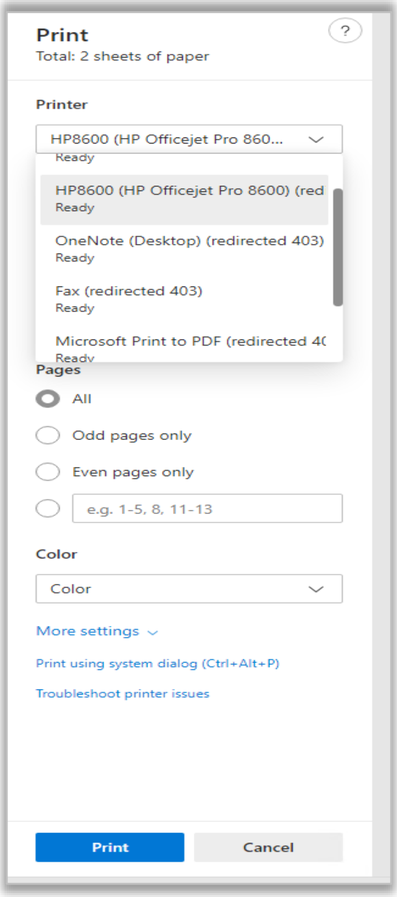
Printing

Maximum number of printers allowed to connect: 10

Verifying Printers are Enabled

To check what printers are available in your remote desktop session, perform the following steps:

1. Open **Notepad** by double-clicking on the Notepad icon on your desktop.
2. Select **File>Print** from the Notepad application menu.
3. In the print window you will see all printers available under Select Printer (see image).



Print
Total: 2 sheets of paper

Printer
HP8600 (HP Officejet Pro 860...
Ready

HP8600 (HP Officejet Pro 8600) (red
Ready

OneNote (Desktop) (redirected 403)
Ready

Fax (redirected 403)
Ready

Microsoft Print to PDF (redirected 4(
Ready

Pages
● All
○ Odd pages only
○ Even pages only
○ e.g. 1-5, 8, 11-13

Color
Color

?
More settings
Print using system dialog (Ctrl+Alt+P)
Troubleshoot printer issues
Print
Cancel

Print Troubleshooting

If you have followed the steps above and have ensured printers are enabled for your remote desktop connection and are still having issues with printing including, printers not displaying in the printers list, printing to a specific printer causes an error, etc., then please contact the Thornberry Help Center with the printer(s) you are having issues with for further assistance.

Refreshing a Laptop

To refresh a client, follow the steps listed within the Operations Manual. The server address used on the refresh page is provided to you by Thornberry. If you did not receive the web address used on the refresh page or do not remember it, please contact the Thornberry Help Center for assistance.

Client refreshes are only allowed from a specified list of locations (IP addresses). Thornberry collects a list of external (static) IP addresses for each customer office network during implementation. All refreshes must occur from within one of the provided networks to be successful. Contact the Thornberry Support Center to request additional networks to the allow list**.**

Managing Access to External Files via Thornberry Hosted Services

Depending on a user's role in the agency or assigned tasks, access to external files is needed. Since access to the NDoc database is through Hosted services, these files are not going to be accessible directly on the server's desktop.

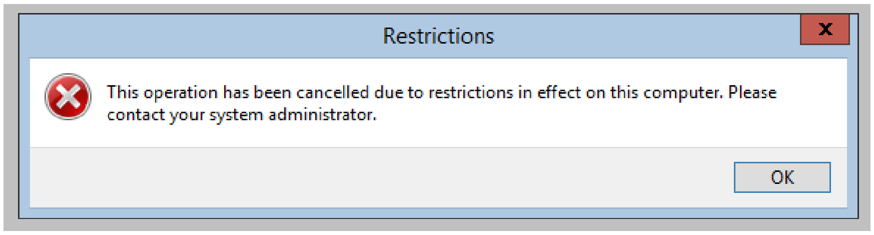
Types of External Access Needs

In general, the circumstances detailed below that necessitate access to external files include but are not limited to:

- **PECOS Import (Administration>System>Agency Settings>PECOS Import):** The CMS list of PECOS enrolled physicians is a file made available to agencies via the Thornberry website. The file is prepared using the data directly from CMS and formatted in a way that can be imported directly into NDoc to keep the PECOS status of physicians within your agency's Physician Table. For details related to the PECOS Import, please refer to the PECOS Import Reference. As with agencies not utilizing Thornberry Hosted Services, the file must be downloaded from the website and unzipped and saved in a method determined by your agency. The file is accessible with your customer Knowledgebase login via the NDoc Updates>Installation Files>CMS PECOS Imports.
- **Document Library (Operations>Document Management>Document Library):** The NDoc Document Library function allows agencies to attach files to a Document Library entry to retain an electronic copy within the patient record (e.g., signed documentation from a physician, consent forms, other internal forms, etc.). Each agency should determine the process for saving these files whether they are saved on a user's internal desktop or a shared drive.
- **OASIS and HIS Files (Administration>System>Downloads):** As part of their daily business, agencies must compile and submit their OASIS and (hospice customers) HIS records to CMS. To facilitate access to these files, Thornberry provides a function that makes OASIS and HIS files available. The function is described in full within the NDoc File Download FASTForm.

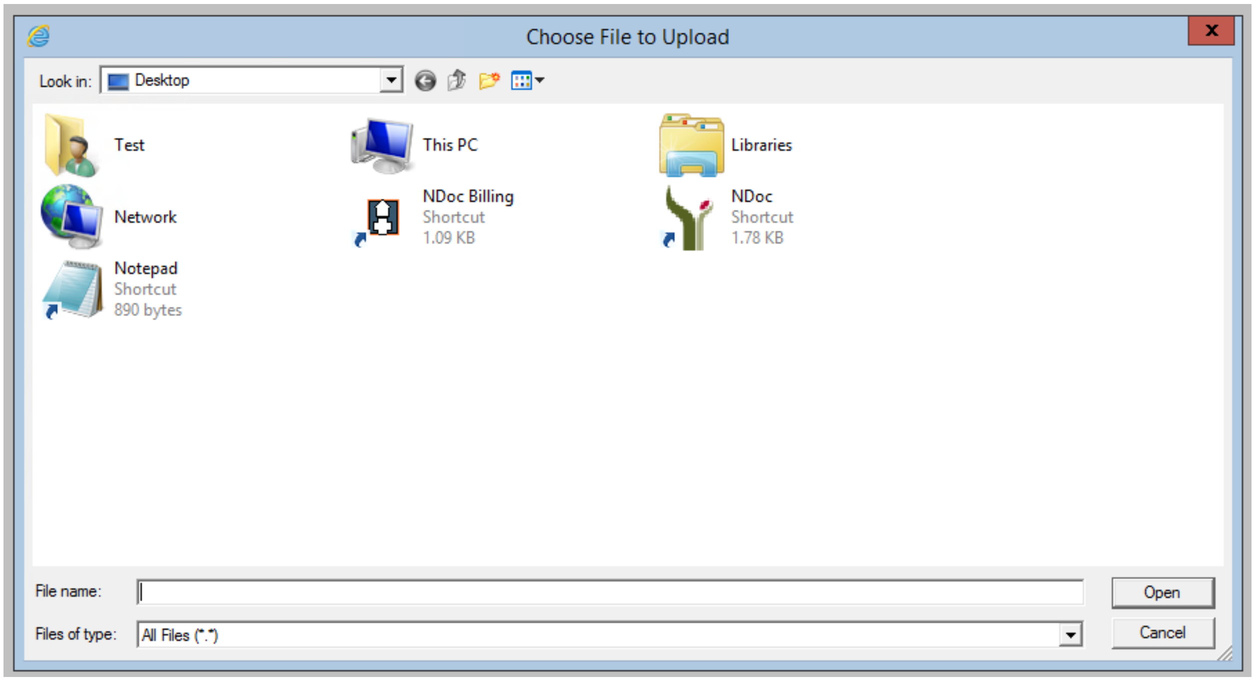
As explained above there are certain situations where an agency needs to access an external file for the purposes of importing or uploading the file directly into the NDoc database. Depending on each agency's pre-determined method for managing their file structure and process for saving files, users should find that when prompted to access files the system will enable the user to access mapped files based on the user's profile permissions. Below are steps to be mindful of during this process.

When prompted to "browse" to a file (e.g., PECOS) or "Add Attachment" (e.g., Document Library), users will receive a message indicating the task is restricted as shown below. Click **OK**.


Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

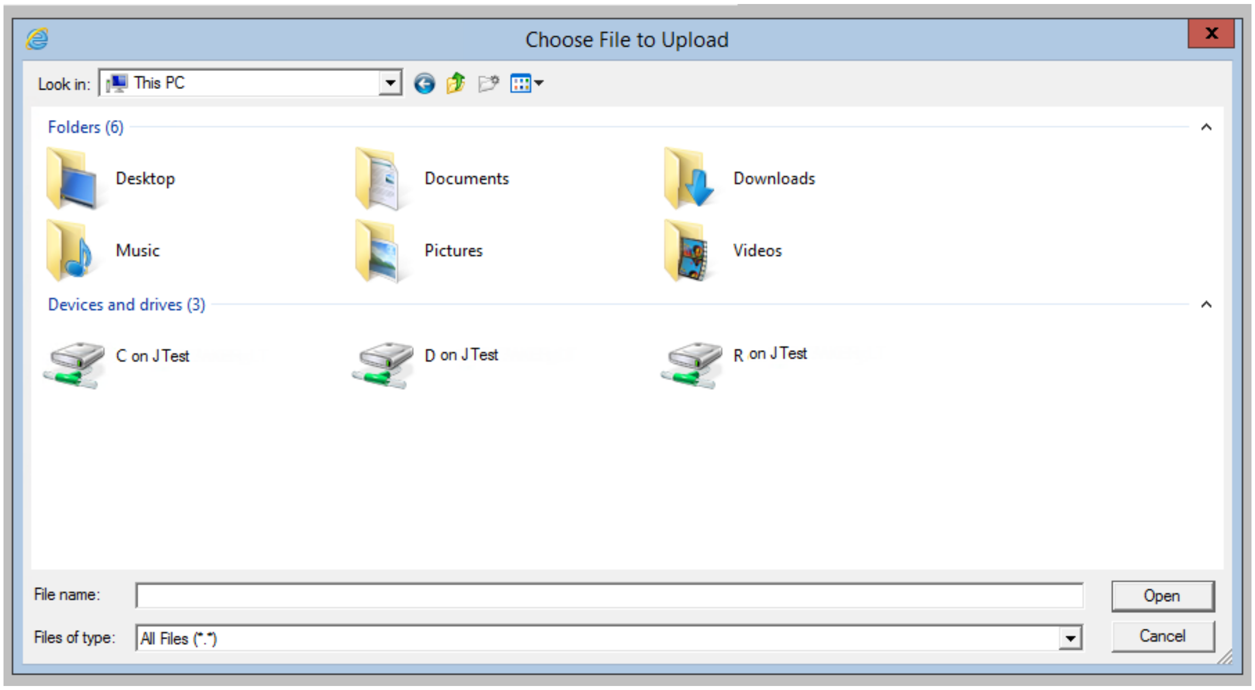
Users will then see their Windows file directory. Depending on the process determined by an agency to save files internally, users will have access to certain files. These are directories mapped to the user's profile. Users should follow the path that brings them to their drive and then the folder where files are located.



Look in: Desktop

Files of type: All Files (*.*)

Go to This PC to access your local machine.

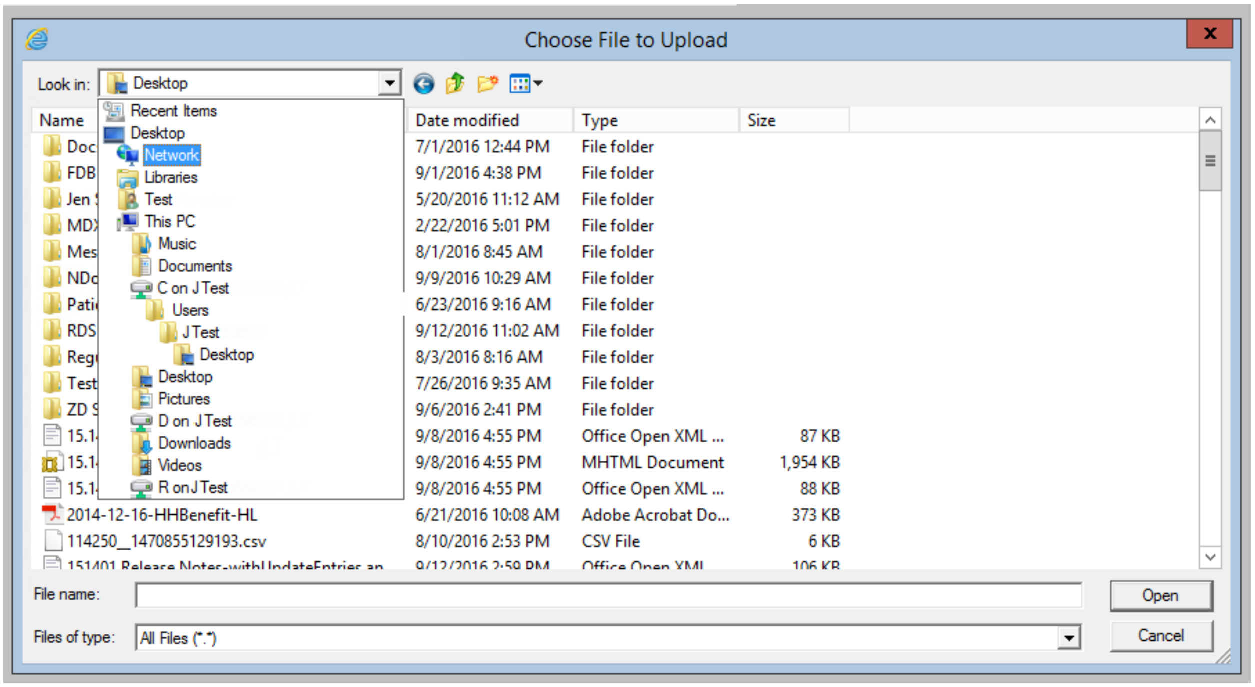


Look in: This PC

Files of type: All Files (*.*)

Choose the appropriate file storage location based on where the file desired is located. In this case, you could select the C Drive and then follow a path to the appropriate file location. For example, if a document is saved on the desktop of J Test, you could follow this path:

Go to This PC>C on JTest>Users>J Test>Desktop, where you will see those items saved to your desktop. *Note when saving files or working with other staff to save files, please note the location for ease of access later.

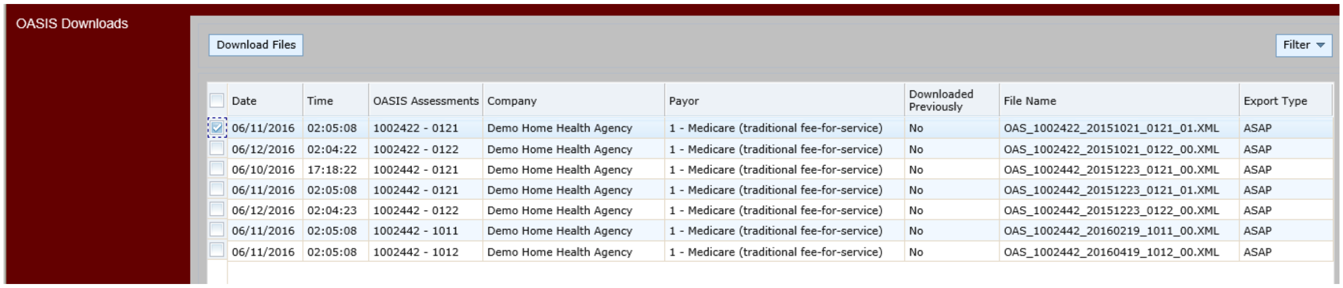


Name	Date modified	Type	Size
Doc	7/1/2016 12:44 PM	File folder	
FDB	9/1/2016 4:38 PM	File folder	
Jen	5/20/2016 11:12 AM	File folder	
MD	2/22/2016 5:01 PM	File folder	
Mes	8/1/2016 8:45 AM	File folder	
NDc	9/9/2016 10:29 AM	File folder	
Pati	6/23/2016 9:16 AM	File folder	
RDS	9/12/2016 11:02 AM	File folder	
Reg	8/3/2016 8:16 AM	File folder	
Test	7/26/2016 9:35 AM	File folder	
ZD S	9/6/2016 2:41 PM	File folder	
15.1	9/8/2016 4:55 PM	Office Open XML ...	87 KB
15.1	9/8/2016 4:55 PM	MHTML Document	1,954 KB
15.1	9/8/2016 4:55 PM	Office Open XML ...	88 KB
2014-12-16-HHBenefit-HL	6/21/2016 10:08 AM	Adobe Acrobat Do...	373 KB
114250__1470855129193.csv	8/10/2016 2:53 PM	CSV File	6 KB
151401 Release Notes-withUpdateEntries an	9/12/2016 2:59 PM	Office Open XML	106 KB

Once the file is selected, click **Open** to start the download or import process depending on the process being executed within NDoc.

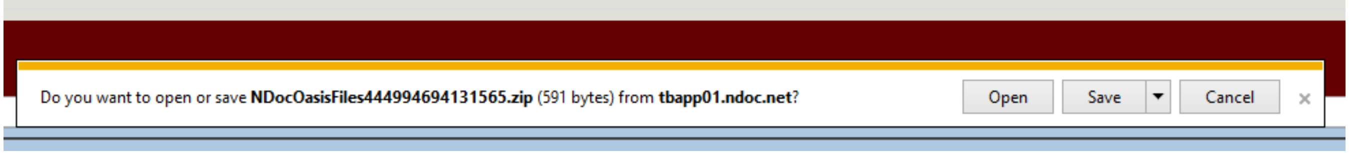
Downloading Files from the Hosted Environment to Your Mapped Drives

In the case of OASIS and HIS Records, users are creating a file to be downloaded to a file location outside of the NDoc Remote Desktop environment. These files are set up as XML files for manual submission to CMS. Once file(s) are selected click the **Download Files** button.



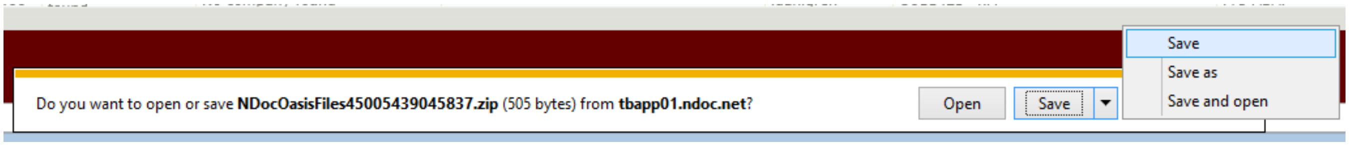
□	Date	Time	OASIS Assessments	Company	Payor	Downloaded Previously	File Name	Export Type
☑	06/11/2016	02:05:08	1002422 - 0121	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002422_20151021_0121_01.XML	ASAP
□	06/12/2016	02:04:22	1002422 - 0122	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002422_20151021_0122_00.XML	ASAP
□	06/10/2016	17:18:22	1002442 - 0121	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002442_20151223_0121_00.XML	ASAP
□	06/11/2016	02:05:08	1002442 - 0121	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002442_20151223_0121_01.XML	ASAP
□	06/12/2016	02:04:23	1002442 - 0122	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002442_20151223_0122_00.XML	ASAP
□	06/11/2016	02:05:08	1002442 - 1011	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002442_20160219_1011_00.XML	ASAP
□	06/11/2016	02:05:08	1002442 - 1012	Demo Home Health Agency	1 - Medicare (traditional fee-for-service)	No	OAS_1002442_20160419_1012_00.XML	ASAP

Users then see a message prompting next steps.



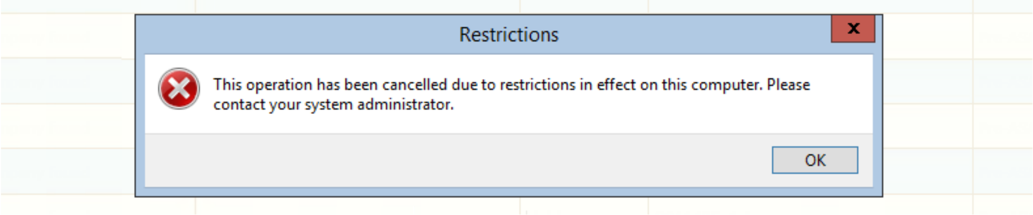
Do you want to open or save **NDocOasisFiles444994694131565.zip** (591 bytes) from **tbapp01.ndoc.net**?

As noted in the File Download Page FASTForm, click **Save As**.



Do you want to open or save **NDocOasisFiles45005439045837.zip** (505 bytes) from **tbapp01.ndoc.net**?

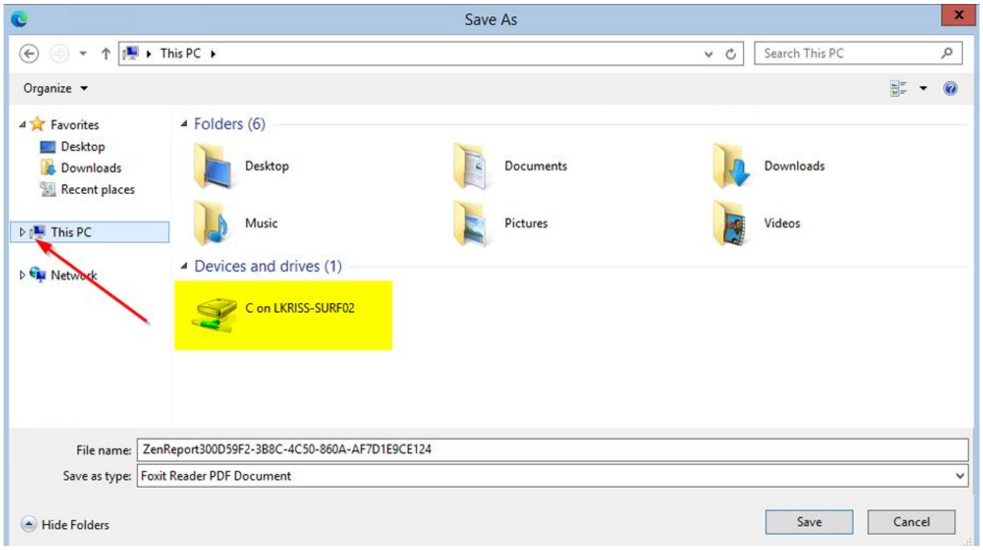
Users will see a Restrictions Error and should click **OK**.



Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

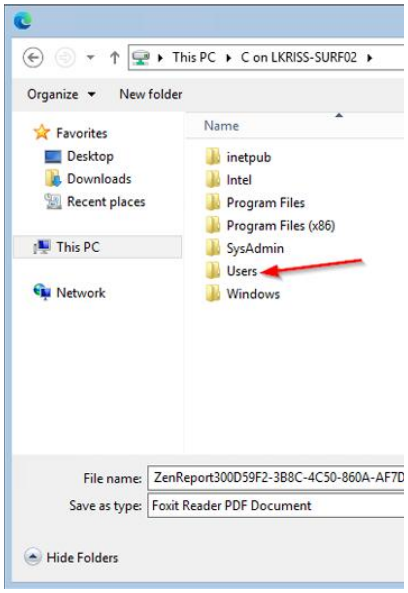
The Windows file directory opens similar to the process of browsing to a file explained above. Choose the appropriate computer and the local mapped drives should display by default. Select and note the location of the files for access at a later time.



Save As

File name: ZenReport300D59F2-3B8C-4C50-860A-AF7D1E9CE124

Save as type: Foxit Reader PDF Document



File name: ZenReport300D59F2-3B8C-4C50-860A-AF7D

Save as type: Foxit Reader PDF Document

Disaster Recovery Outline – Hosted Customers

Purpose

This document defines the current policy for backing up system and electronic information/data within Thornberry Hosted Services for the purpose of recovering critical systems and services in case of data loss or system failure.

Scope

This policy applies to internal systems located in the hosted data center, managed by Thornberry Ltd. which comprise the Thornberry Hosted Services environment.

Key Definitions

Recovery Time Objective (RTO)	Target time to recover from a disaster. Time will vary based on the size of the environment.
Recovery Point Objective (RPO)	The point in time to which systems and data can be restored after a disaster. Time is measured from the point of disaster.
Full Backup	A backup in which all of a defined set of data objects are copied, regardless of whether they have been modified since the last backup
Internal/Infrastructure Components	Components that make up the core structure of the hosted environment, including the backup systems
Snapshot	Full disk image changes between snapshot operations - provides a fully functional copy of the environment at that particular point in time.

Detail

Systems and Utilities

Windows: An appropriate backup solution will be used to perform backup and recovery operations of operating system and non-operating system data.

Healthshare: Healthshare’s built-in backup utility will be used to perform database backup and recovery of NDoc Clinical databases. The backup utility creates a flat file that is then backed up with the system image.

SQL Server: SQL Server’s built in backup utility will be used to perform database backup and recovery of NDoc Billing databases. The backup utility creates a flat file that is then backed up with the system image.

Production Backup Schedule

Backup Window: Healthshare backups are conducted daily during off peak hours, typically around 12:30 am (local time zone). System snapshot backups are taken six times a day for application servers, including during peak business hours. System snapshot backups are taken daily for Remote Desktop servers, during off peak hours. SQL Server backups are performed twice daily, including during peak business hours.

Full Backup: Each system snapshot backup taken has the capability to bring a fully functional system back online with data consistent as of the time the snapshot was taken.. Each snapshot is considered a full backup. There are no incremental backups performed. System snapshots taken will have no noticeable impact on system usage or performance.

HealthShare backups taken have the capability to bring the NDoc database back to the data point at which the backup was taken. Each backup is a full backup of the databases on the server. When HealthShare backups are taken, there will be significant system usage and performance degradation that can be expected.

SQL Server backups have the capability to restore a NDoc Billing database back to the data point at which the backup was taken. Each backup is a full backup of each database on the server. When SQL Server backups are taken, there will be no noticeable impact on system usage or performance.

Validation

Snapshot backup jobs are verified to ensure each has completed successfully at every interval. Backup jobs that fail are rescheduled for the next available interval.

HealthShare backups are checked to ensure completion. Thornberry Ltd support will be notified if the backup fails. Backups that fail are investigated and resolved so that the following day's backup executes successfully.

SQL Server backups are checked daily for successful completion. Backups that fail are investigated and resolved so that the next scheduled backup executes successfully.

Test restoration of data will be conducted at least annually. Each application server will be restored during that time at the discretion of the Thornberry Ltd management staff and a support representative will validate application functionality and data integrity at the recovery point.

Exclusions

At this time, no systems are excluded from the backup process.

Data Recovery

Data that is damaged or deleted can normally be restored within 4-6 hours (see Backup Overview Matrix) depending on the amount of data to be recovered and the nature of the damage/failure. Disaster recovery procedures from backup sets within the last seven days may be initiated by the appropriate executives at the agency, and once approved by Thornberry Ltd. management, will be performed by the appropriate Thornberry Ltd support representative (NDoc or NDoc Billing databases only).

Backup/Recovery Summary Matrix

Component	Environment	Recovery Time Objective	Recovery Point Objective	Backup Type	Schedule
Active Directory (Windows Logon)	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours
DNS	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours
IIS (Domain Controller)	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours
HealthShare (Domain Controller)	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours
SQL Server	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours
IIS (Application Servers)	Production	Up to 4.5 hours	Up to 4 hours	Full	Every 4 hours
HealthShare (Application Servers)	Production	Up to 4.5 hours	Up to 4 hours	Full	Every 4 hours
Remote Desktop Services	Production	Up to 5.5 hours	Up to 4 hours	Full	Every 4 hours

All backups are stored for 7 days at the hosted data center, with a copy of the backup stored off site.

Maintenance

In the data center where Thornberry Ltd is responsible for maintenance, internal/infrastructure components will be managed in accordance with the Memorandum of Understanding.

Memorandum of Understanding: Server Maintenance and Updates

In order to ensure NDoc and the hosted environment it resides in is secure and running at peak performance, the hosted environment requires a monthly maintenance program. These steps are critical to ensuring the integrity of your system and keeping NDoc up to date with the latest features and patches. Agencies opting to utilize a Thornberry Ltd. hosted server solution are not responsible for the maintenance of the server or the installation of monthly updates. These tasks are provided as part of the Thornberry Ltd. hosting solution by members of the Thornberry Ltd. support team. To prevent any unintended interruptions to your service, agencies are hereby notified that Thornberry Ltd. will schedule server maintenance and update installations on the **fourth Monday of every month between the hours of 11:00 PM and 2:30 AM EST.** An email will be issued to the primary customer contacts upon completion of maintenance each month. Additionally, automated install of any Sub-Minor update (customers will be notified via email on the date of install) will occur at 12:15 AM (according to customer timezone). Users will receive in-application messaging five minutes prior to the install, and at 12:15 AM will be automatically logged out of NDoc. Customers will be prevented from accessing NDoc for no more than fifteen minutes while the Sub-Minor update installs.

Additionally, Thornberry will perform a monthly cleanup/review of inactive RDP sessions to match current licensing availability. A portion of the email confirming completion of maintenance will include a list of all currently active RDP users and a request to reply with any that are no longer active.

Prior to the installation of a monthly update, agencies should recognize the importance of preparing for changes to the NDoc system. In an effort to limit any disruption in functionality, please adhere to the following set of guidelines.

- □ Agencies should promptly read the Release Notes for the monthly update.
- □ Agencies should participate in the monthly NDoc webinar designed to review the content of the monthly update.
- □ Agencies should provide adequate notice of any functionality changes to **ALL** users prior to the monthly update.
- □ Agencies MUST instruct **ALL** users to log off the system for the duration of the maintenance and update install.

Questions regarding the monthly maintenance and update installation process should be directed to the Thornberry Help Center.