

NDoc Software

Thornberry Hosted Services Manual

Copyright 2024 Thornberry Ltd. All rights reserved.

NDoc® is a registered trademark of Thornberry Ltd. All rights reserved.

This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without the prior written permission of Thornberry Ltd.

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 4
Connecting to NDoc within the Hosted Environment 5
- Configuring Multi-Factor Authentication for MyApps Access 5
- Connecting Using MyApps Connection 5
- Opening NDoc and NDoc Billing 8
- Remote Desktop Logoff Procedure and Reconnection 9
- Password Policies 10
- Changing the Password Options: 10
- Changing the Remote Desktop Password from the Desktop 11
- Forgotten Password/Locked Account 11
- Password Expiration 12
- Terminal Session Handling 13

Printing 14
- Verifying Printers are Enabled 14
- Print Troubleshooting 14

Refreshing a Laptop 15
Managing Access to External Files via Thornberry Hosted Services 16
- Types of External Access Needs 16
- Downloading Files from the Hosted Environment to Your Mapped Drives 18

Disaster Recovery Outline – Hosted Customers 20
- Data Protection & Backups 20
- Disaster Recovery Approach 20
- Security & Compliance 20
- Testing & Continuous Improvement 20
- Customer Communication 21
- Summary 21

Memorandum of Understanding: Server Maintenance and Updates 22

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.

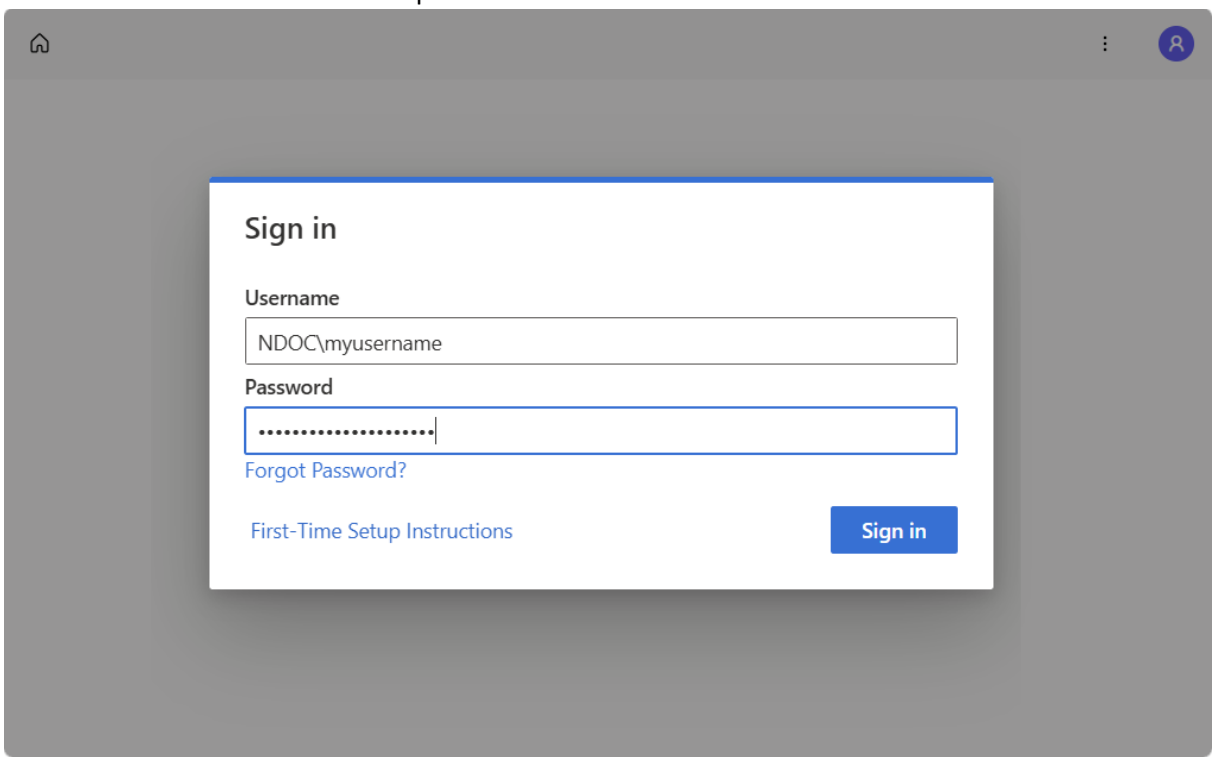
Configuring Multi-Factor Authentication for MyApps Access

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.

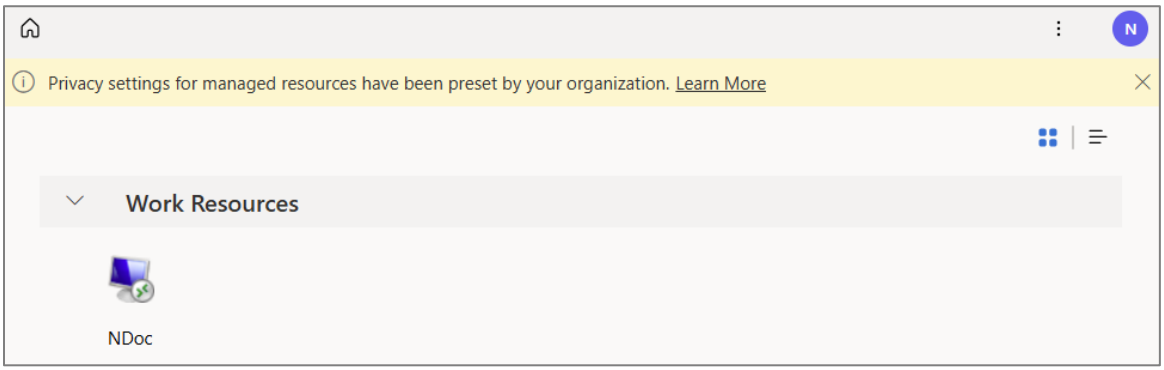
Connecting Using MyApps Connection

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.

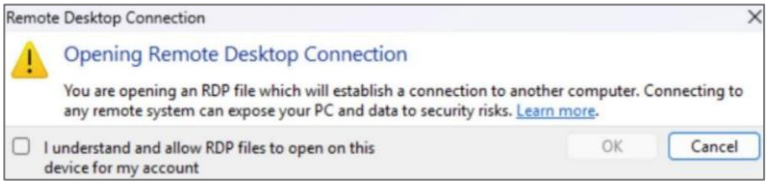


You will land on the main page to launch the NDoc Desktop Application. Click the **NDoc Desktop Icon** to open and access desktop functions.



NOTE: As the result of an April 2026 Windows Update (April 14, 2026—KB5083769) some users encountered new prompts when attempting to connect to a Remote Desktop (RDP) session via MyApps. **Please read this notice in full for important information about downloading a new RDP File.**

These changes appear to be related to enhanced security measures and may require users to take a few additional steps during connection. After the installation of the Windows update, users may see the following prompt before completing the MFA process:



Users should check the confirmation and click **OK**.

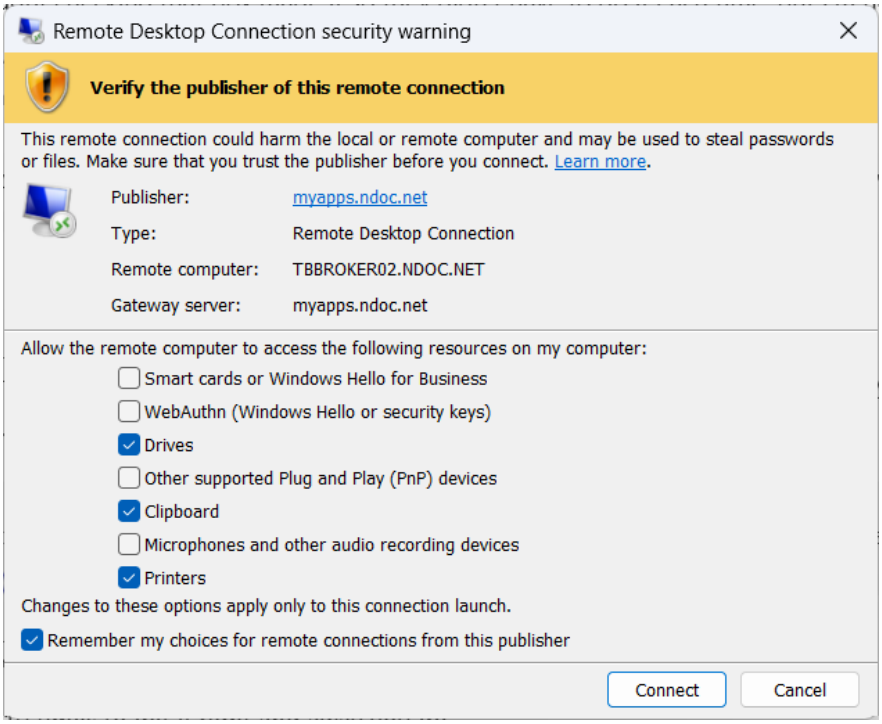
Users will see the next prompt below:

Users should confirm the Remote Computer reflects *TBBROKER02.NDOC.NET* and the Gateway Server reflects *myapps.ndoc.net*.

To ensure that mapped services are retained, users should check the following under the "Allow the remote computer to access the following resources on my computer" options:

- Drives
- Clipboard
- Printers
- Remember my choices for remote connections from this publisher

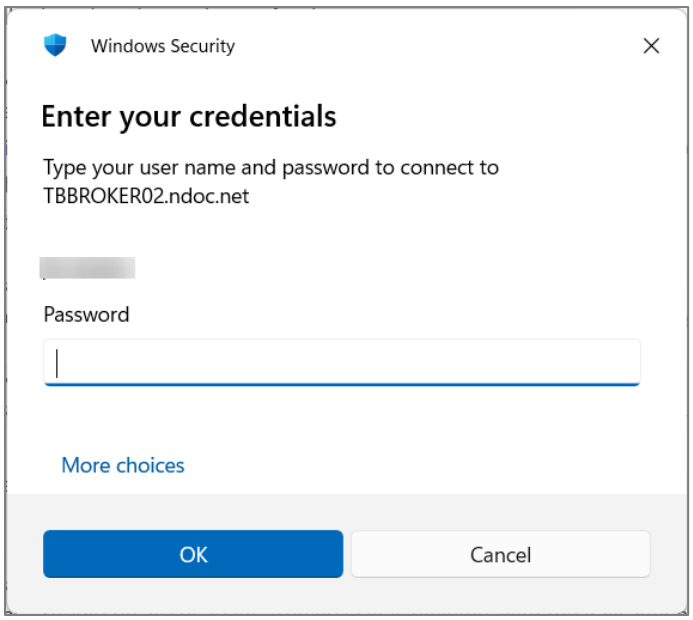
Users should then be able to connect to proceed.



***NOTE**: To provide the best possible user experience, we have updated the RDP File available at https://myapps.ndoc.net/ to be digitally signed so that users can remember their choices for which local resources should be available within the RDP session. Many customers download this file once and share it with all users, or individual users download the file once and re-use each time they connect. We recommend that everyone be sure to download the latest RDP File available. Additionally, the file will need to be updated every six months when the signing certificate expires and is updated to a new certificate. The current expiration schedule will have our next certificate update occurring in the June/July timeframe. While the original file will still work, users will not see the checkbox option to remember their choices.*

NEXT

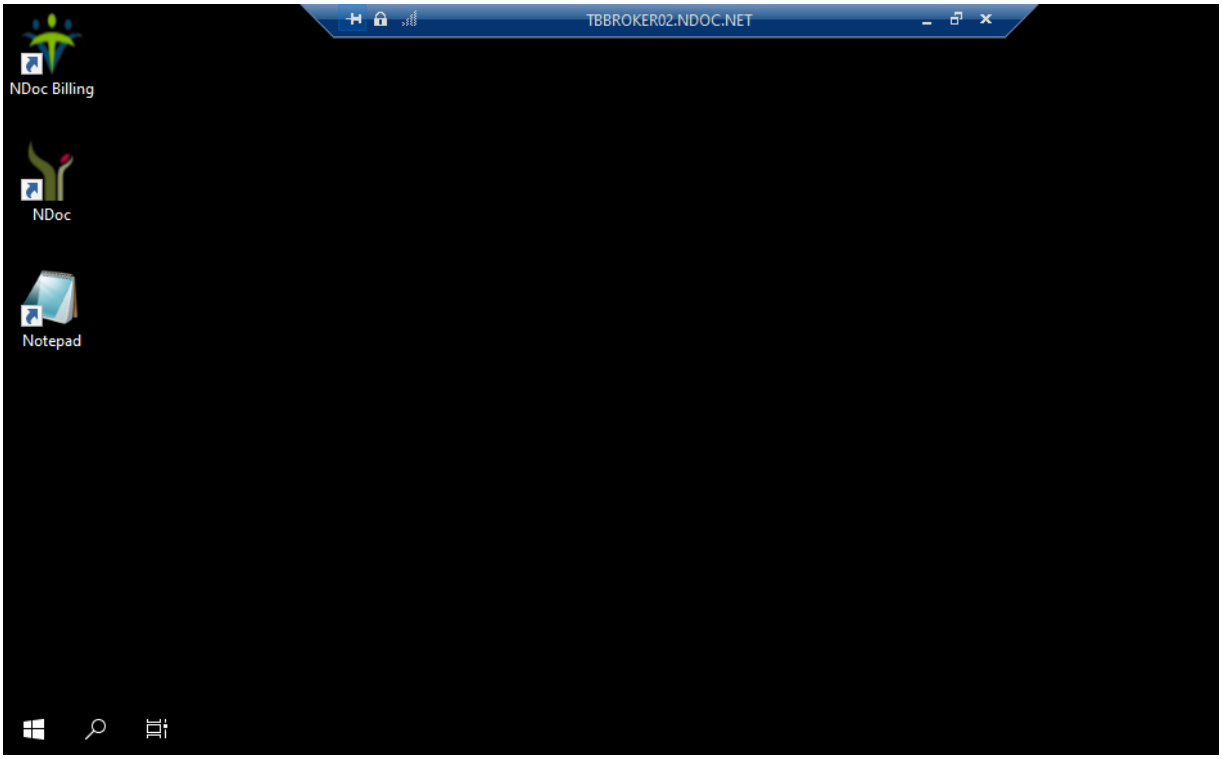
Depending on the browser, users will see a prompt to download/open the RemoteApps file. When the download occurs, users are again prompted with a security pop-up to again enter their credentials:



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.

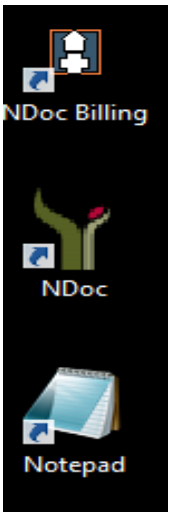


After the remote desktop session loads, a Windows desktop displays (*see image below*).



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

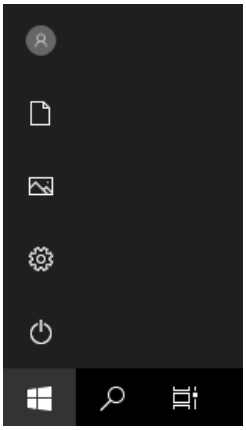
There are multiple ways to exit a remote desktop session; one will cause the session to remain open for a period of time on the server so that you can reconnect to it and the other will perform a normal Windows log off procedure for the session, making the session no longer available for reconnection.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

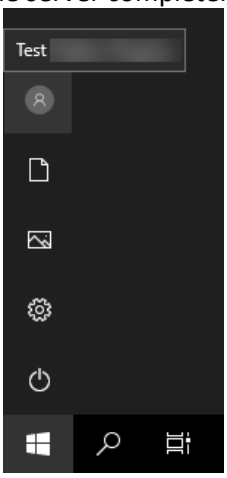
The first method can be accomplished by hovering with the mouse pointer at the top-center of the screen until a dropdown appears. The dropdown contains the normal Windows buttons for minimize, maximize/restore, and close. Clicking the **X** button will *disconnect* your session.

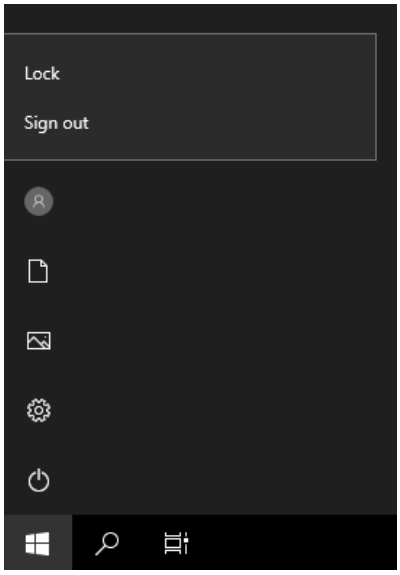


Another way to exit a remote desktop session is to click the **Start Menu** button (Windows icon) in the bottom left corner and open the menu to see the User icon. Hovertext will appear to identify the user. Click the icon and then click **Sign out**. This will close the session on the server completely

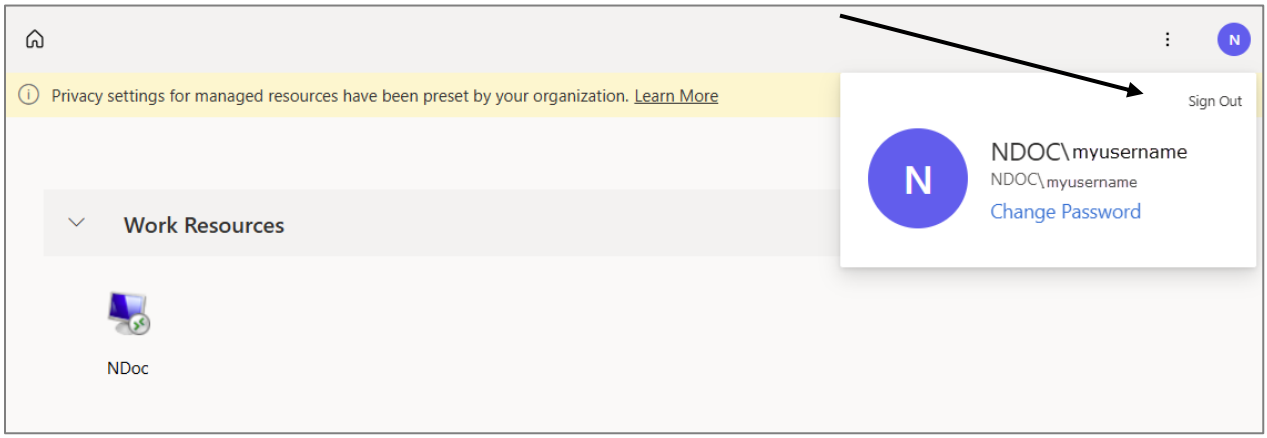








In addition to the process of signing out of the remote session, users may also take the step of signing out of the MyApps session using the **Sign out** option within the profile menu accessible on the top right side of the screen.



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

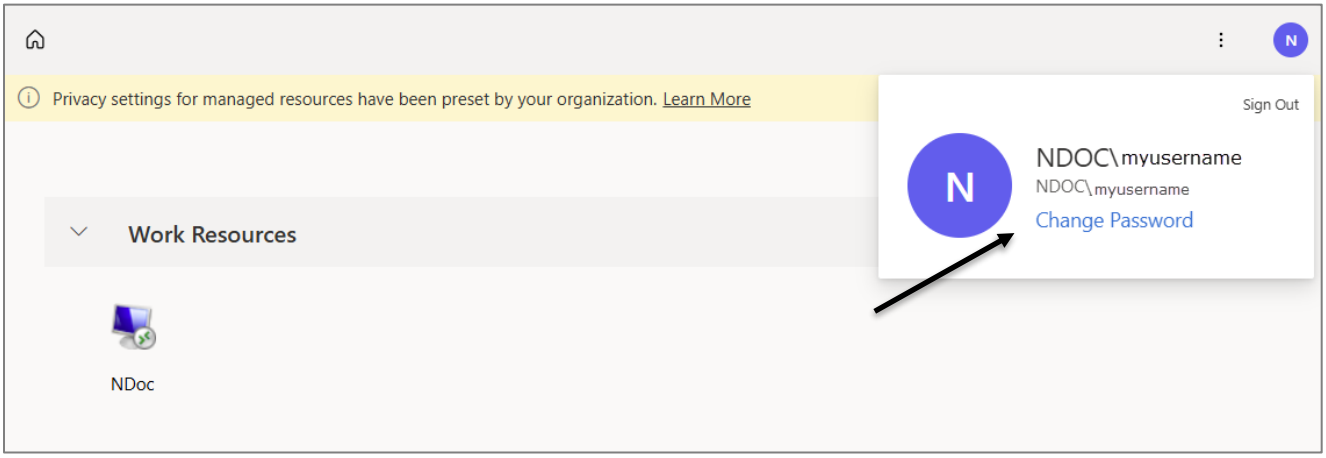
If for any reason a password needs to be reset, please review the "Forgotten Password/Locked Account" section of this manual for instruction. Should use of that functionality prove ineffective, an authorized Help Center user should submit a request directly to the Thornberry Help Center. The support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

Changing the Password Options:

Users have two options to initiate a Change Password action. Below are the two options:

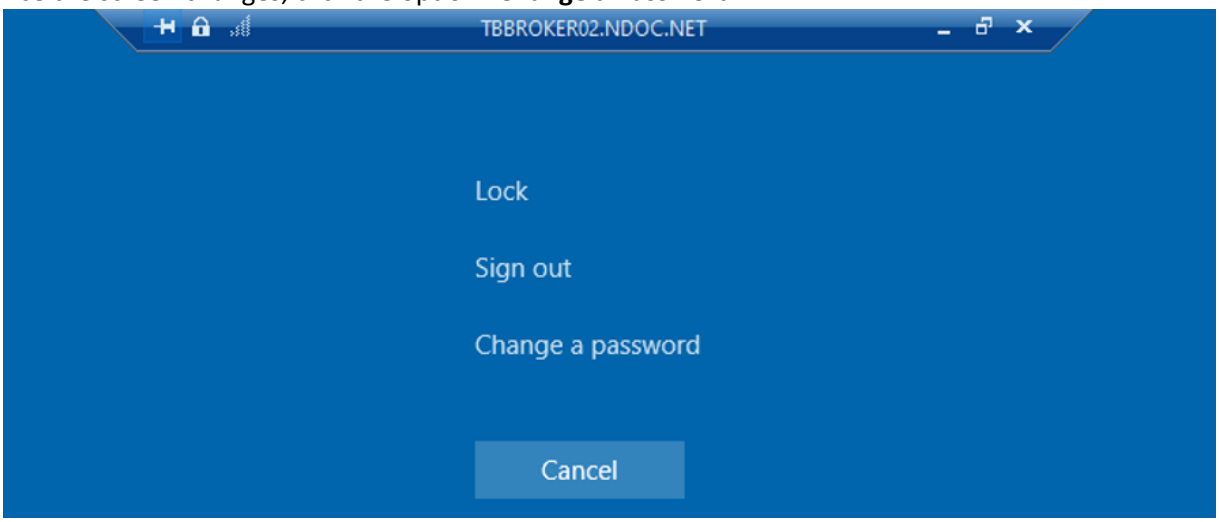
Changing the MyApps/Remote Desktop Password from the MyApps login page

1. Open the user profile in the top right corner.
2. Click the Change Password option.
3. This will trigger the Password Reset process as described later under *the Forgotten Password/Locked Account* section.



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

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."

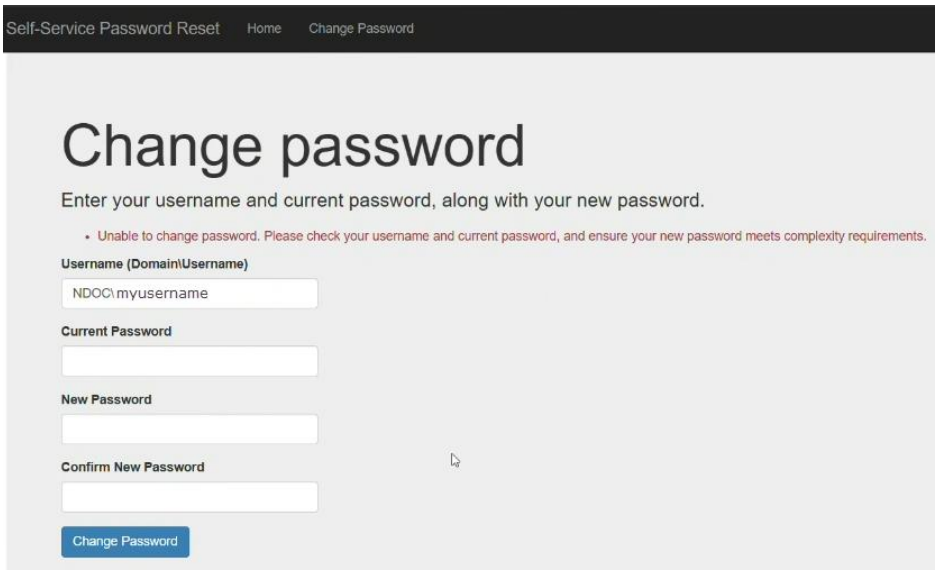


2. After clicking "Reset Password," the "Password reset initiated" message (below) will display to alert the user to watch for an email to their registered email address.
3. After receiving the "Password reset initiated" messaging, if an email is associated with the user, they will receive an email from bot@thornberryltd.com at their registered email address indicating:

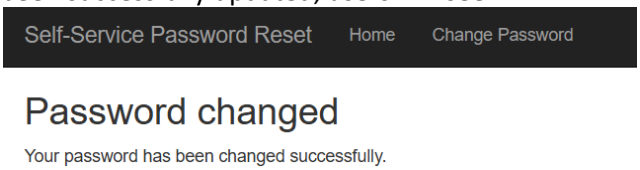


"Your new temporary password is:
[new temporary password]
You will be asked to change the password the next time you log in to the system."

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.

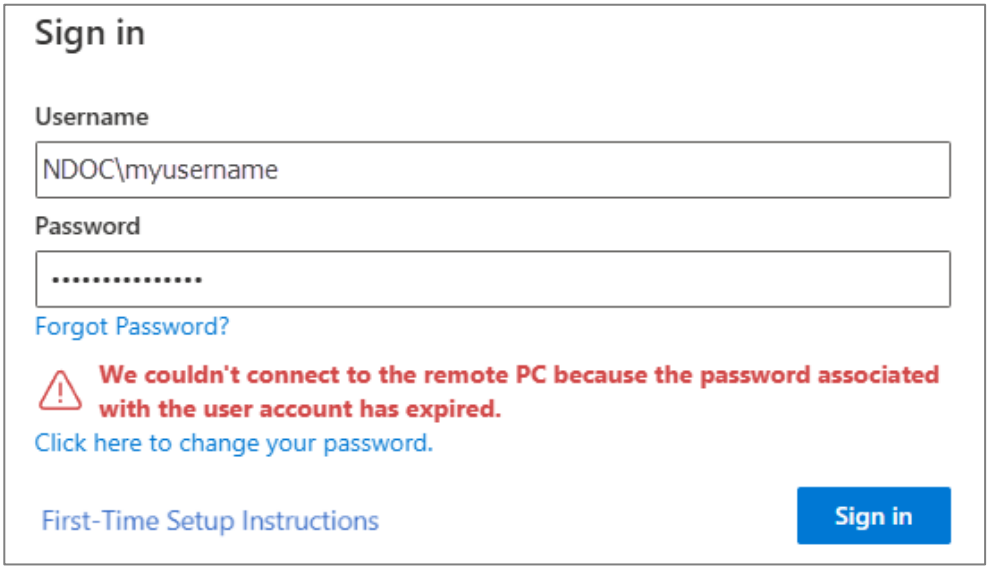


When the new password has been successfully updated, users will see:



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.



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.

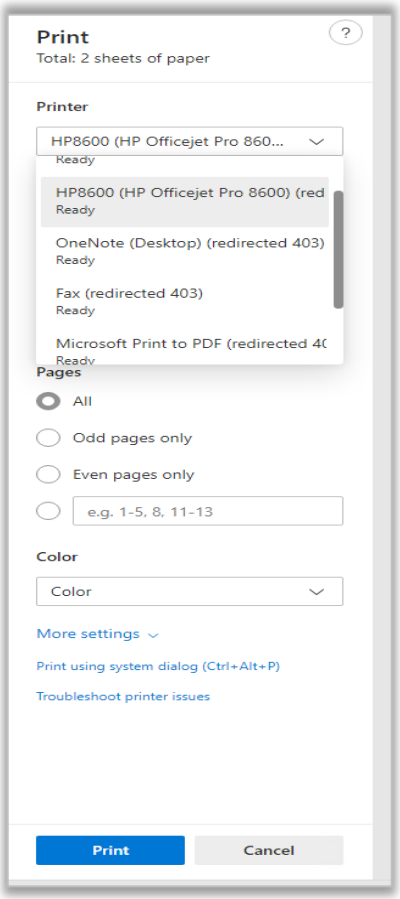
Printing

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 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.

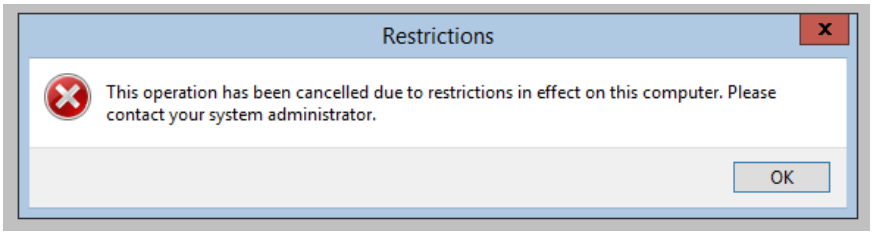
Types of External Access Needs

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

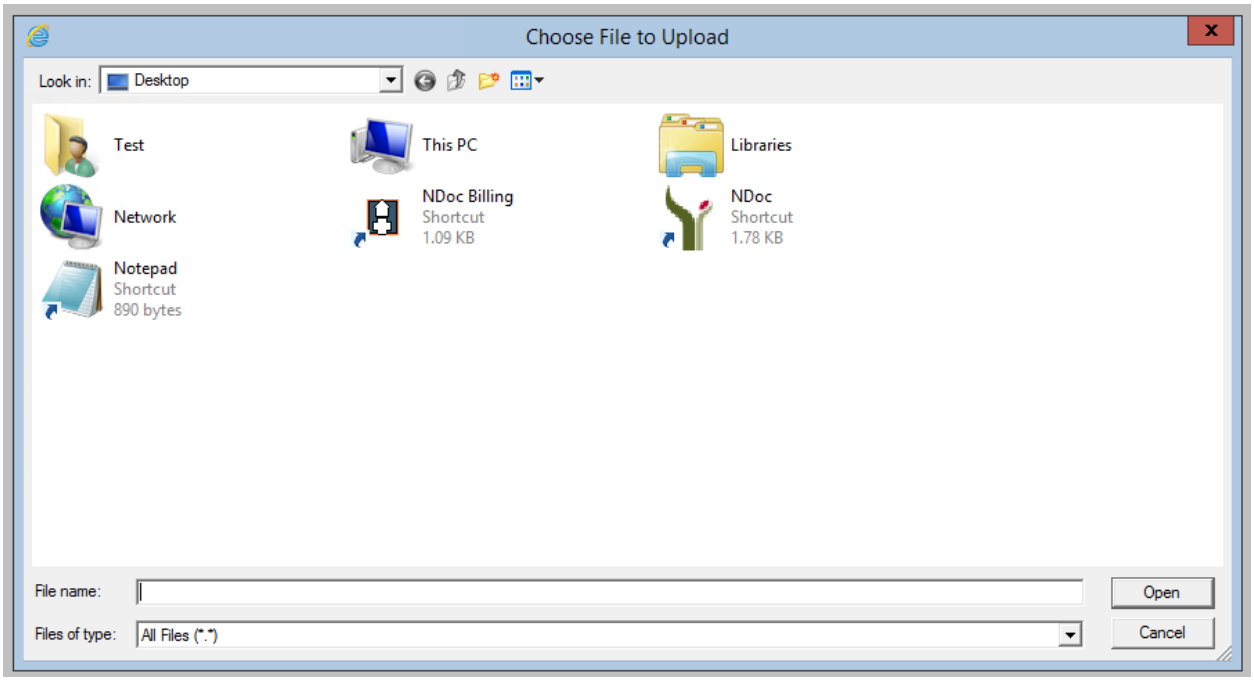
- **PECOS Import (Administration>System>Agency Settings>PECOS Import):** The CMS list of PECOS enrolled physicians is a file made available to agencies via the Thornberry website. The file is prepared using the data directly from CMS and formatted in a way that can be imported directly into NDoc to keep 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.

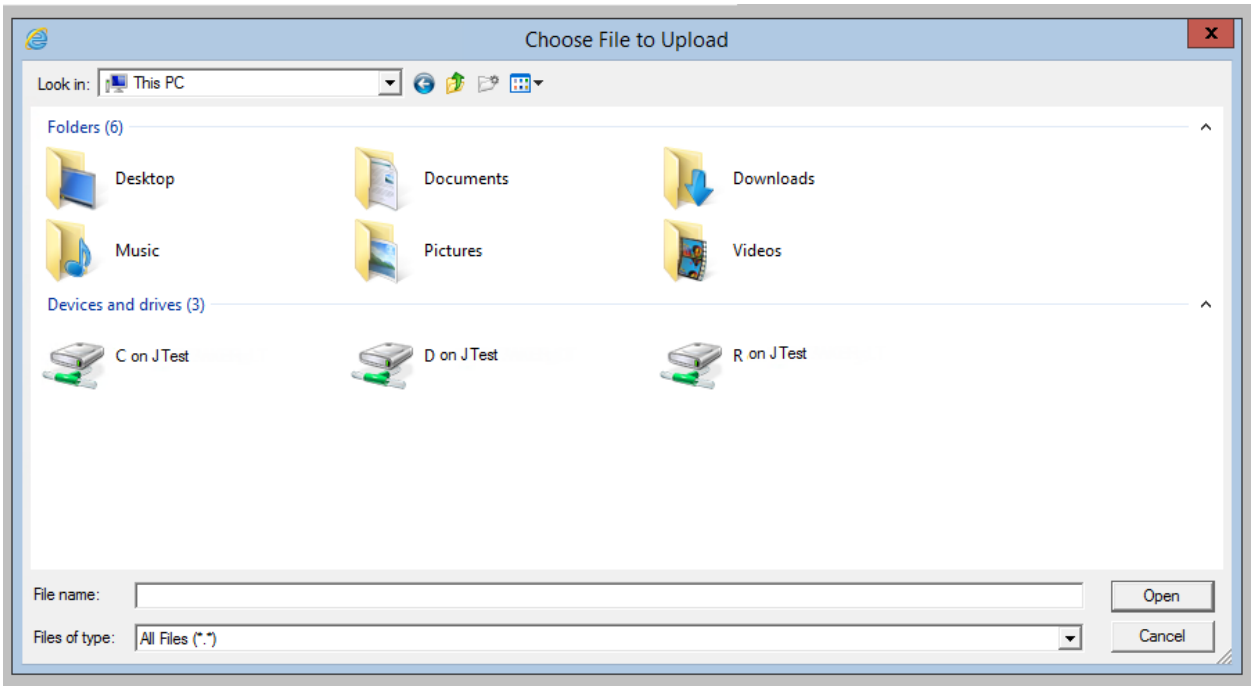
When prompted to "browse" to a file (e.g., PECOS) or "Add Attachment" (e.g., Document Library), users will receive a message indicating the task is restricted as shown below. Click **OK**.



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.

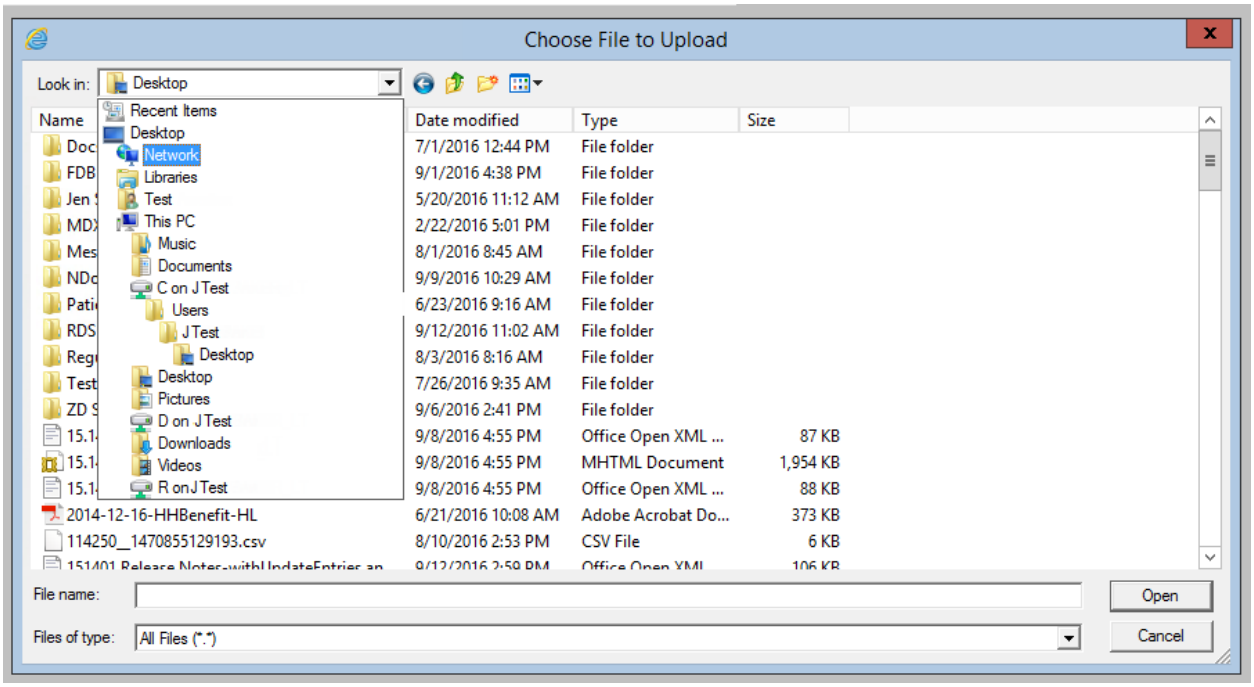


Go to This PC to access your local machine.



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.



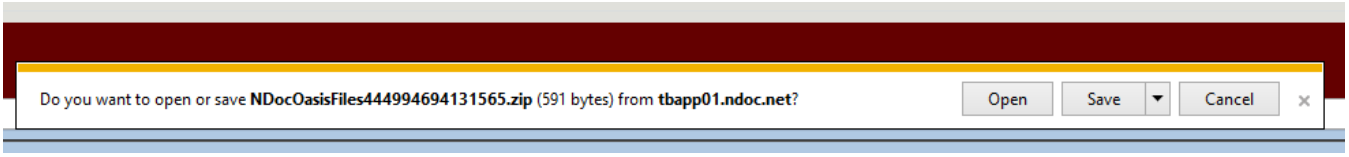
Once the file is selected, click **Open** to start the download or import process depending on the process being executed within NDoc.

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.



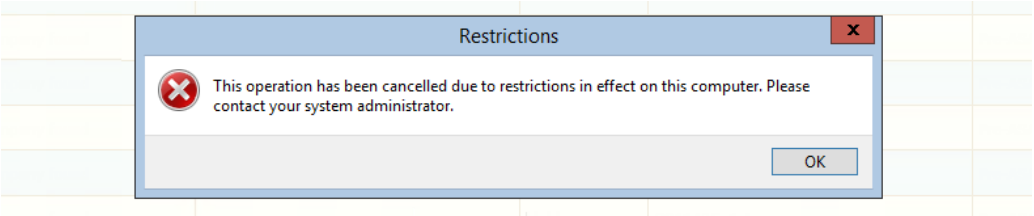
Users then see a message prompting next steps.



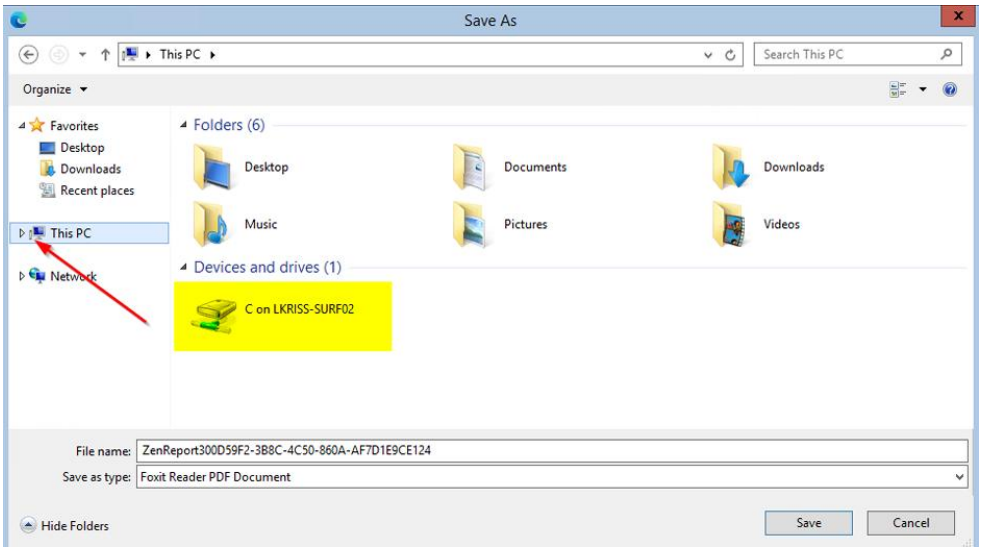
As noted in the File Download Page FASTForm, click **Save As**.

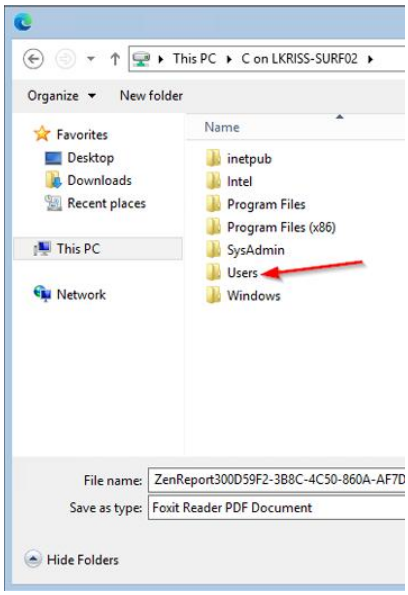


Users will see a Restrictions Error and should click **OK**.



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.





Disaster Recovery Outline – Hosted Customers

Data Protection & Backups

To protect customer data, we implement the following controls:

- Automated backups every 4 hours using AWS Backup
- Application-consistent (VSS-aware) backups for Windows-based systems, including databases
- Encryption at rest and in transit
- Secure storage and retention of backup data within AWS

These measures ensure that data can be reliably restored to a consistent state in the event of failure or data loss.

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

Disaster Recovery Approach

Our disaster recovery strategy is based on backup and restore procedures, designed to rapidly rebuild the production environment in the event of a major incident.

In a declared disaster scenario, our team will:

1. Provision a clean and secure recovery environment within AWS
2. Restore critical systems from the most recent valid backup
3. Re-establish system connectivity and application services
4. Validate system integrity and data consistency
5. Restore customer access and resume normal operations

Recovery procedures are executed by trained personnel following documented runbooks.

Security & Compliance

We are committed to protecting sensitive healthcare data and maintaining compliance with applicable regulations, including HIPAA.

Key controls include:

- Encryption of data at rest and in transit
- Role-based access controls and least-privilege principles
- Audit logging and monitoring of system activity
- Controlled access to backup data and recovery processes

Testing & Continuous Improvement

Our disaster recovery procedures are regularly reviewed and tested to ensure effectiveness.

- Periodic internal testing and validation exercises
- Ongoing updates to reflect infrastructure or application changes
- Continuous improvement based on test results and operational experience

Customer Communication

In the event of a service disruption, Thornberry will provide timely and transparent communication, including:

- Incident status updates
- Estimated time to recovery
- Confirmation of service restoration

Summary

Thornberry is committed to maintaining a resilient and secure platform for our customers. Through a combination of reliable backup strategies, defined recovery objectives, and tested procedures, we ensure that critical systems and data can be restored within established timeframes.

For additional information, please contact the Thornberry Help Center.

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 ET.** 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.