



Account Creation & Management

**A Guide for Voluntary Agency
Security Administrators**

July 2020

Table of Contents

- I. Obtaining the Necessary Accounts and Permissions.....4**
 - Step 1 - Obtain Regular User Accounts on both the HSEN and SVC Domains5
 - Step 2 - Register your Regular Accounts and Passwords on the NYS ITS Password Self Service Portal 5
 - Step 3 – Obtain SSL-VPN Permission.....6
 - Step 4 - Acquire an RSA Token7
 - Step 5 - Submit Requests for Creation of HSEN Administrative and SVC Special Access Accounts9
 - Step 6 - Register your Administrative Accounts and Change Passwords on the Self-Service Portal...12
 - Step 7 – Access the NYS Landing Page via SSL-VPN13

- II. WebStar..... 16**
 - Accessing WebStar16
 - Creating a User Account18
 - Adding CONNECTIONS Application Access23

- III. The ARS (Active Roles Administration) Application 26**
 - Accessing ARS26
 - Navigating within ARS28
 - Password Resets in ARS31
 - Administrative Password Resets in ARS.....32
 - Workers Who Leave: Deprovisioning Accounts in ARS32
 - Re-Enabling (Reprovisioning) an Account34
 - Unlocking an Account35

- IV. Troubleshooting Log on and Other Issues..... 40**
 - Pulse Secure40
 - You Are Not Allowed to Sign In Error.....43
 - You Do Not Have Permission to Login Error44
 - Could Not Retrieve Your User Record Error (WebStar and/or ARS links are greyed out).....45
 - Invalid Username or Password Error Message45
 - HTTP Error 401.1 – Unauthorized Error Page46
 - Site Can't be Reached or Can't Reach this Page47

This Site is Not Secure/Problem with Website’s Security Certificate Error47

The Active Directory Administration Fields Do Not Display in WebStar48

You Do Not Have Local Security Administrator (LSA) Permissions (WebStar)49

WebStar Error 8007085a.....49

Unable to Re-access WebStar after Creating a New Account and being Knocked Out of the Application.....50

No Groups Display in ARS51

There are No Resources Currently Available for This User52

SSL Error 4.....53

Acknowledgements

This guide was produced by the New York State Office of Children and Family Services CONNECTIONS Team with assistance from the New York State Information Technology Services and our Voluntary Agency partners. Thanks to the following staff for their contributions:

- | | |
|--------------------------------------|--|
| Janet Brown, OCFS CONNECTIONS | Jennifer Buchanan, ITS Customer Relations |
| Christina Calderon, OCFS CONNECTIONS | Jennifer Fill, ITS |
| Linda Gorthy, OCFS CONNECTIONS | Kenroy Grant, ITS |
| Timothy Payne, OCFS CONNECTIONS | Andrea Rohan, ITS |
| Thomas Werle, OCFS CONNECTIONS | Michelle Walker, Liberty Resources LSA |
| Sandra Wilson, OCFS CONNECTIONS | Victoria Savard, Mountain Lake Academy LSA |

Obtaining the Necessary Accounts and Permissions

There are several accounts, applications and permissions needed by a Voluntary Agency Local Security Administrator (LSA) to successfully access the NYS network and complete their duties. These include the following:

- **A user account on the HSEN domain** (your “regular” account to log into CONNECTIONS), typically two letters and four numbers, such as 6972XX or AD7802
- **A regular user account on the SVC domain** (same format as your HSEN ID)
- **An administrative (ADM) account on the HSEN domain** (used to access features within the WebStar application when creating accounts for other users or adding access to the CONNECTIONS application).
- **A Special Access account on the SVC domain** (used to access features within the ARS application to manage user accounts once they have been created in WebStar)
- **SSL-VPN permission** to access state applications such as WebStar, ARS and Cognos/Data Warehouse from a non-state-owned device (e.g., an agency owned computer)
- **an RSA token** - needed for two-factor security authentication when accessing applications on the NYS network. Tokens may be either hard (fob) or soft (codes sent you via an application on your phone or other device)
- **an up-to-date version of the Pulse Secure application** on the device you will use to access the state network.

Note: A transition to the ARS application is currently underway. Once completed, an ADM account on the HSEN domain will no longer be needed as all account creation and management activities will be done in ARS.



Administrative and Special Access account requests to NYS-ITS are now handled electronically via the ITSM application. Since Voluntary Agency workers do not have access to the ITSM system for creating electronic requests, this step is done by the CONNECTIONS Implementation Team.

Detailed instructions are included in this guide for CONNECTIONS Team Members to accurately complete electronic requests in the ITSM system. Voluntary Agency users can disregard instructions shown in this format.

The creation of accounts and granting of permissions still require the completion of several forms, as noted in the steps below. **Forms must be completed, printed, signed, scanned and returned electronically to your CONNECTIONS Implementation Team member for processing.**

It is important that each of these account creation steps be completed in the correct order.

Step 1 - Obtain Regular User Accounts on both the HSEN and SVC Domains

Regular user accounts on both HSEN and SVC domains are needed before the administrative accounts needed to access WebStar (HSEN domain) and ARS (SVC domain) can be set up.

When a regular HSEN account is created, it should auto-migrate to SVC domain within 24 hours.

Note to CONNECTIONS Team Members:

*You must request the establishment of **BOTH** regular accounts (HSEN and SVC) via the ITSM Self Service Portal>Service Catalog>User Accounts and Access>User Account Access.*

If you do not request the SVC account, it will not be set up and will prevent the later creation of the SVC Administrative account needed to access ARS.

The regular account MUST have a valid email address connected to it that displays in the Global Address List (GAL). This is required in order to create the administrative accounts and email ID, password and password reset instructions to the user. The email address listed will also link all three accounts together so that they can be deprovisioned as a group when the time comes.

If a user is new to CONNECTIONS, does not have a regular account, and the agency does not currently have a Local Security Administrator (LSA) who can create one, a request can be made to OCFS-ITS by your CONNECTIONS Implementation Team member to have one created. This is currently handled by Paula Ainspan at the OCFS Home Office.

The following user information is needed to create a regular account:

- First Name
- Last Name
- Middle Initial (if available)
- Work Address
- Work phone number
- Email address
- Job Title
- Agency name (as shown in the Resource Directory)
- Agency code
- Agency site code (if multiple sites)

Once the regular accounts are created, the user will receive an email listing their new account ID and a temporary password. **Users should log onto the network with each to activate the account and to complete a required first-time log on password change.** Temporary passwords expire in 72 hours, so users should log on as soon as they receive their new accounts and temporary passwords.

Step 2 - Register your Regular Accounts and Passwords on the NYS ITS Password Self Service Portal

Additionally, all users should register their accounts on the NYS ITS Password Self-Service Portal (<https://password.ny.gov>) to expedite future password resets. Even though the two regular accounts look similar, they are two separate accounts, and each must be registered on the portal.

Hint: It may be helpful to set both passwords as the same.

When registering accounts, Voluntary Agency staff should not use their email address. Instead, use your domain (HSEN or SVC), followed by a backslash (\) and your CONNECTIONS ID (e.g., 6972XX). Thus, for example, “HSEN\6972XX” and “SVC\6972XX”. Accounts on **BOTH** domains should be registered.

Note: Reset the password for your HSEN domain account first. Sometimes, when you reset the HSEN\UserID account it automatically syncs to the SVC\UserID account and sets the same password for that account. If you then attempt to change the SVC\UserID account password, you will be alerted that passwords cannot be changed more than once in 24 hours. This indicates that new HSEN\UserID password has already synced to the SVC\UserID account and both now carry the same password. If you receive this message, cancel the password change for the SVC\UserID account.

To test this, go to Manage My Passwords section in the portal, which will prompt you for your current password. Enter the password you just set for the HSEN\UserID account as the password for the SVC\UserID account. If it works, cancel and do not proceed with any change for this account.

Step 3 – Obtain SSL-VPN Permission

Once the regular HSEN account has been created, SSL-VPN access must be applied for by completing the SSL-VPN request form (OCFS-4827), available at <https://ocfs.ny.gov/help/remote-access/#t1-Remote-Access-Requests> under the section for *Information on Secure Socket Layer Virtual Private Network (SSL VPN) for Non-State Owned Equipment*.

This form has recently been revised (11/26/19) and simplified, but it still must contain the signature of the Voluntary Agency’s Executive Director. Per the OCFS Legal Department, *electronic signatures or emailing the form from the account of the Executive Director cannot be substituted for a physical signature*.

Print the form, complete it, have it legibly signed by the agency’s Executive Director, scan it and return the completed electronic copy to your CONNECTIONS Implementation Team member so it can be submitted via the ITSM system (a process currently managed by Jennifer Wright at OCFS Home Office).

Note: SSL-VPN requests for Cognos (Data Warehouse) access should be emailed directly to the data.warehouse@ocfs.ny.gov address as noted on the form. They do not go through ITSM.

Note to CONNECTIONS Team Members:

SSL-VPN requests are submitted via the ITSM Self Service Portal>Service Catalog>User Accounts and Access>User Account Access

- ***In the **Short Description** field:*** Enter the name of the VA user and their regular user account, stating that they need SSL-VPN access.
- ***In the **Description Field:***** restate the name and regular account of the user needing SSL-VPN. Add the reason why - i.e. "Needs to access WebStar and ARS to create new accounts and maintaining user accounts for (Name of Agency and Agency code)".
- Choose Peter Whitford as the **Approver**.
- In the **Select appropriate NYS Entitlements** section, click the SSL-VPN Access and the Data Access boxes.
- **Attach** the signed, scanned SSL-VPN request form.
- Click the **Order Now** button.



Note: After the request has been submitted, you must also email Pete Whitford (Peter.Whitford@ocfs.ny.gov) to alert him that the request is awaiting his approval.

Step 4 - Acquire an RSA Token

An RSA token is required to securely access the state network from a non-state-owned device (such as an agency-owned laptop or computer) via SSL-VPN.



You must have a regular user account and SSL-VPN access before applying online for a token.

1. Navigate to the RSA website, <https://mytoken.ny.gov>

2. As your **User ID**, enter your state issued email address (@dfa.state.ny.us) ***if you have one.***

NEW YORK STATE OF OPPORTUNITY | Office of Information Technology Services | SELF-SERVICE CONSOLE

Home

This application is used to manage your token usage. Your User ID is typically in the form of your email address.

Log On

Log on with your corporate credentials to request new tokens and manage existing tokens.

User ID

Forgot your user ID? Contact your administrator.

Support

[Troubleshoot SecurID token](#)

Do you need to enable a new token?
[Enable your token](#)

3. For workers who do not have a state issued email address (i.e., who are “Custom Recipients” and use an agency email address), this field will need to be completed with one of the 6 choices below. If one does not work, please try the next choice until one does.

- [userid@ext.ny.gov](mailto:user@ext.ny.gov)
- [userid@dfa.state.ny.us](mailto:user@dfa.state.ny.us)
- Firstname.lastname@dfa.state.ny.us
- [userid@hsen.ny.gov](mailto:user@hsen.ny.gov)
- Firstname.Lastname@hsen.ny.gov
- Firstname.Lastname@ext.ny.gov



If none of the above choices work, the email address associated in the background with your account doesn't fit a usual pattern. **Please call the Enterprise Service Desk at 844-891-1786 or email them at FixIt@its.ny.gov for assistance.**

4. If you can successfully log in, follow the steps in the RSA SecurID Token Request User Guide, available at https://its.ny.gov/sites/default/files/documents/rsa_token_request_job_aid.pdf to complete your token request.

- **Note:** Your “Office 365 password” is the password for your CONNECTIONS account, not necessarily the one you use to log into your agency computer.

Step 4: Enter your Office365 Password <i>(this is the same password you use to log onto your computer and email) and select Log On.</i>	<p>Log On</p> <p>Logon is required. If you have forgotten your logon information, contact your help desk or administrator.</p> <p>User ID: edward.donnelly@its.ny.gov</p> <p>Authentication Method: Password</p> <p>Password: [Masked]</p> <p>Cancel Log On</p>
---	---

- Be sure to include the email address that you typically use so that you can receive communications relevant to your request.
- If ordering a hardware token, be sure the street address on file is correct so that your token can be mailed to you without delay. The address field pre-fills with the address listed for you in the NYS Global Address List (GAL), to which voluntary agency workers do not have access. If the prefilled address not correct, be sure to enter the one where you want the token mailed.
- If you have applied for but not received your token within a reasonable amount of time, please contact the Helpdesk for follow up at 844-891-1786.
- Typically, requests for soft tokens are fulfilled much more quickly than those for hard tokens.

A Further Note about Tokens:

- Tokens user specific: they are associated with a user's email and, for soft tokens, phone number. Therefore, they CANNOT be transferred between users.
- When a user who has been issued a hard token no longer needs it, the agency's LAN Administrator should physically obtain the token from the user and mail it back to NYS ITS at the following address:

Dawn DeZago
P.O. Box 2062
Albany NY 12220
- For soft tokens, the LAN administrator should email the user's information to hs.crm@its.ny.gov. The Customer Relations Management (CRM) staff will send the information to the RSA Administration staff.
- Tokens cannot be re-enabled once they are collected and sent back. A new token will need to be ordered for a user who has left the agency and returned.
- If a user is having issues with their token, the user themself can reset their credentials on the <https://mytoken.ny.gov> website or call the Helpdesk for assistance.

Step 5 - Submit Requests for Creation of HSEN Administrative and SVC Special Access Accounts

Once regular accounts have been established, SSL-VPN permission received and an RSA token acquired, requests for an administrative account on the HSEN domain (for WebStar) and a special access account for the SVC domain (for ARS) can be requested.



Administrative/Special Access account requests must be submitted via the ITSM system with the assistance of your CONNECTIONS Implementation Team member as Voluntary Agency workers do not have access to the ITSM portal.

Complete the AD Admin Request Form (updated 2/6/19) available on the Forms page, under Security Forms on the CONNECTIONS internet webpage.

Please be sure you use the most recent version of the form and fill it out in its entirety. It will be rejected if not completed fully. If you are unsure of the terminology, ask your CONNECTIONS Implementation Team member for assistance.

- Print the form and have it signed (legibly) by the Agency's Executive Director. Per the OCFS Legal Department, *electronic signatures or emailing the form from the account of the Executive Director cannot be substituted for the physical signature.*
- Scan the completed, signed form and email the electronic copy to your CONNECTIONS Implementation Team member so it can be submitted via the ITSM system.

Note to CONNECTIONS Team Members:

Administrative account requests are submitted via the ITSM Self Service Portal>Service Catalog>User Accounts and Access>Active Directory (AD) Privileged & Service Accounts

Two different units at ITS are involved in the creation of SVC Special Access accounts:

- **L2 EUS UAM** creates the SVC account with the format of *_(firstinitial)(lastname)*
- **L2 Plat Enterprise AD** adds the SVC\ *_(firstinitial)(lastname)* account to the correct groups

While the completed form must be attached to the request, all information on the form must also be included in the narrative section of the ITSM online request (RITM) as ITS



staff do not refer to any attached forms. The forms are used for OCFS Legal tracking purposes only.

For example:

“Mary Jones (HSEN\AD7802 and SVC\AD7802) is the new LAN Administrator for Abbott House (P10), a voluntary agency that uses the OCFS CONNECTIONS application. She needs an Administrative account created on the HSEN domain to access WebStar (LSA group) and a Privileged 9Special Access) account created on the SVC domain to access ARS (Full Control group). Mary’s email address is MJones@Abbotthouse.net.”

Complete the form information as follows:

- **Agency Name** – as shown under “Site Information” on the form

Site Information Provide the address of the new user’s location
Agency Type Check one: <input type="checkbox"/> County <input type="checkbox"/> Voluntary
Site ID: _____
County or Voluntary Agency Name: _____
Street Address: _____
City: _____ State: _____ ZIP: _____ Phone: _____

- **Users first and last name** – as shown on the form under “Important Note”

IMPORTANT NOTE: ADM users must have an existing valid email address in the GAL, associated with their Non-Admin account before an Admin account can be created and this request processed.
Clearly list the new ADMIN user(s) names
Last Name: _____ First Name: _____ Email: _____
Last Name: _____ First Name: _____ Email: _____
Last Name: _____ First Name: _____ Email: _____

- **Email address** where new/existing admin's info should be sent – as shown on the form under “Important Note”
- **Existing User ID(s)** – this is the “regular” accounts created on the HSEN and SVC domains.

- **Group membership** the admin will need – shown on the form under “Security Roles Description”

The only group on the HSEN domain that should be chosen is the LSA group.

- An LSA (Local Security Administrator) can create accounts for new users and add access to the CONNECTIONS application.
- An LSAA (Local Security Administrative Assistant) used to be able to unlock regular user accounts and reset passwords in WebStar. **All account management** – including resetting passwords and unlocking accounts - **must now be done in ARS**, so this role is no longer needed in WebStar.
- SO (Server Officer) and WO (Workstation Officer) – are not roles needed by Voluntary Agency staff since they do not manage equipment on the NYS network.

Security Roles Description – check all boxes (groups) below that the new Admin account should be a member of

Add to LSAs Group
Local Security Administrators (LSA) permission to provision Admin and Non-Admin accounts

Add to LSAA Group
Local Security Assistant Administrator (LSAA) permission to reset a Non-Admin user's password

Add to SOs Group
Server Officer (SO) permission to log into and administer servers in Active Directory

Add to WOs Group
Workstation Officer (WO) permission to administer workstations in Active Directory

Groups on the SVC domain must also be specified in the request:

- *ARS Full Control Administrators - allows management of user accounts, workstations, servers (similar to a combination of HSEN LSAs, SOs, WOs) as well as password resets*
- *ARS UserHelp Desk - only allows password resets*
- **Be sure the Executive Director's signature is complete and legible** in the Authorizer Information section of the form so ITS can confirm the request is coming from the proper person.

Authorizer Information - Person authorizing this request must be the Executive Director or the Commissioner (Electronic signatures will **NOT** be accepted)

Signature: _____

UserID (Domain\UserID): _____ Email: _____

Full Name (Last, First): _____ Phone: _____

Title: _____

Address: _____

Once administrative and special access accounts have been created, the user will be alerted by email (hence the need to include the correct email address).

- The user may need to check their Junk email folder to be sure the incoming message has not been inadvertently diverted.
- The email will contain the two new ADM accounts.

- Temporary passwords for each will be emailed to the user separately for security reasons.
Temporary passwords expire in 72 hours.

Unlike regular accounts, the administrative accounts on HSEN and special access accounts on SVC MAY NOT use the same format.

- HSEN Administrative accounts typically have the format of “ADM(regular user ID)” (example, “HSEN\ADM6972XX”).
- Some existing SVC Administrative accounts may use the same format of “ADM(regular user ID)” (example: “SVC\ADM6972XX”)
- More recently created SVC Administrative accounts use a format of “(underscore)(first initial)(last name)” (example: “SVC_JBuchanan”).

Reminder: HSEN Administrative accounts are ONLY used WITHIN WebStar. SVC special access accounts are ONLY used to access and manage accounts in ARS.

Step 6 - Register your Administrative Accounts and Change Passwords on the Self-Service Portal

It is important to sign on to newly created administrative accounts as soon as you receive the new accounts and temporary passwords as these passwords will expire within 72 hours.

To change your passwords, go the NYS ITS Password Self-Service Portal at <https://password.ny.gov/>.

- Use your temporary password as the current password.
- Be sure to register BOTH the administrative account and the special access account and complete security questions for each.

Hint: While you will have four separate accounts (HSEN regular, SVC regular, HSEN administrative and SVC special access) it is helpful when navigating in WebStar and ARS to have your administrative/special access account passwords match your regular account passwords. ***You will still need to manage them as separate accounts even if they have the same passwords.***

Passwords must meet the following complexity requirements:

- Cannot contain all or part of the user’s account name
- Must be at least 8 characters long
- Must contain characters from the following 3 categories
 - ✓ English uppercase characters (A through Z)
 - ✓ English lowercase characters (a through z)
 - ✓ Numerals (0 through 9)



Note: While ITS policy allows the use of non-alphabetic characters (e.g., !, \$, #, %) in passwords, you cannot successfully log into WebStar or ARS with a password that contains such characters. Do not use them.

- You cannot reuse your last 13 passwords.

- Six invalid attempts to sign on to the network will result in a **locked** account.

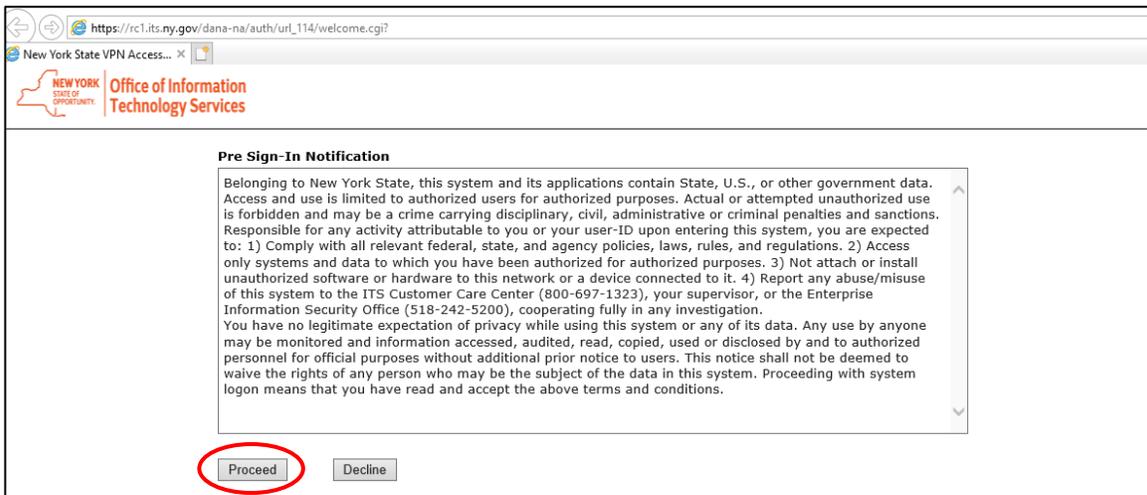


Note: ADM passwords expire every 60 days. Regular account passwords expire every 90 days.

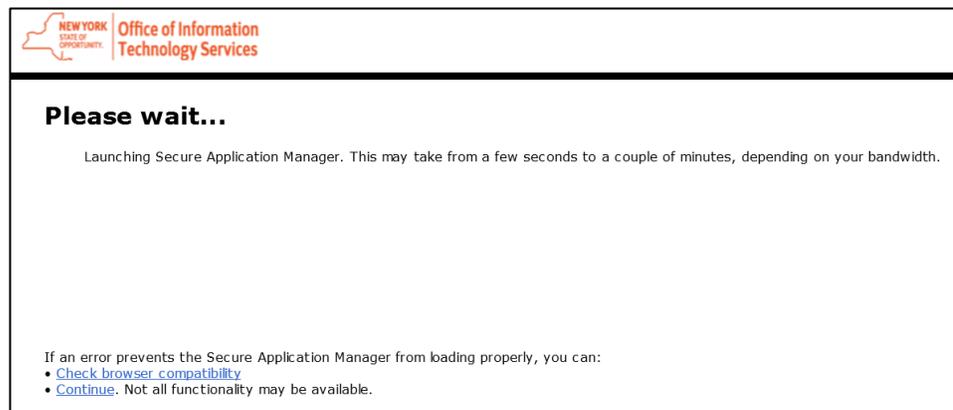
Step 7 – Access the NYS Landing Page via SSL-VPN

After a user has received their new HSEN and SVC administrative accounts and successfully changed the temporary passwords on the Self-Service Password Portal site (password.ny.gov), the next step is to log onto the SSL-VPN landing page to access WebStar and ARS.

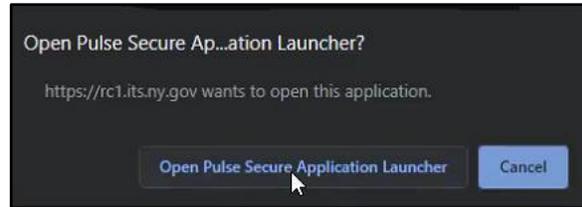
1. Log on to <https://rc1.its.ny.gov/svc> to reach the NYS landing page that contains links to the state applications to which you have been given access (e.g., WebStar, ARS, Cognos). **The only way to reach these applications is via this landing page.**
2. On the Pre Sign-In Notification page, after reading the disclaimer, click the **Proceed** button.



You will receive a message that components are loading. This may take a while, depending on the speed of your internet connection.



If you are asked if you wish to Open the Pulse Secure Application Launcher, click the **Open** button.



If you are asked if you wish to download the software, click the **Always** button.

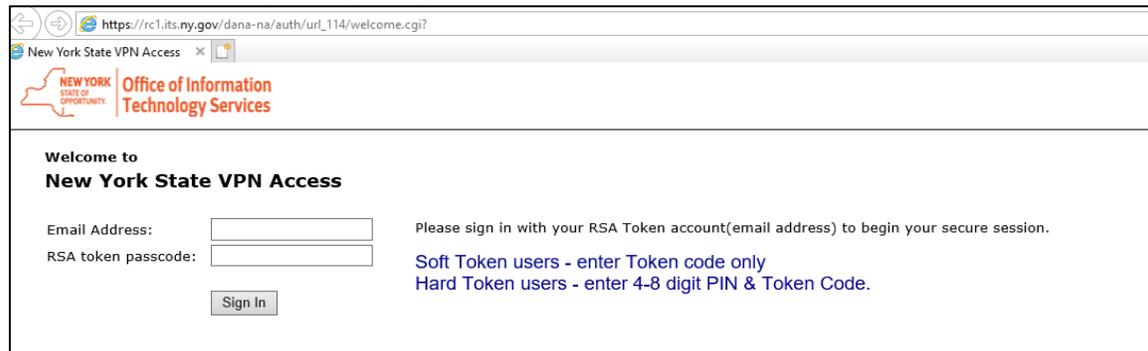


Installing software would typically be the responsibility of the Voluntary Agency's IT staff as users do not generally have the administrative rights needed to install software on their own computer.

The components should then load.

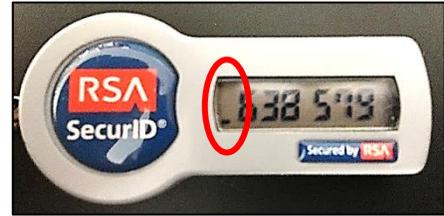


3. On the log in page, enter the email address used when you set up your token account. ***This may not be the email address your regularly use.***



4. Enter your RSA token code.
 - If you are using a hard token, you must enter the PIN you created when you activated your token, followed by the token generated code (no spaces between).

- Hint: New codes generate every 60 seconds. If the dots on the left side of the fob (one for every 10 seconds) show as almost ready to expire, wait for a new code to generate before attempting to log in.
- Soft tokens only require entry of the generated code (no PIN).



5. Click the **Sign In** button.

The landing page will display the list of applications for which you have been granted access permission.

Click on a link to access the application.



If you encounter problems logging in to the chosen site, see Section IV - Troubleshooting Log In Issues, beginning on page 40 of this document for additional assistance.

WebStar

WebStar is a legacy application that is slowly being phased out by ITS. Once used to create and manage user accounts and to manage servers and workstations on NYS domains, it is now used **ONLY** to create user accounts. **You cannot manage user accounts or reset passwords in WebStar even though these options still appear to be available.** All user account management (provisioning and deprovisioning accounts, moving users between groups, unlocking accounts, resetting passwords) must now be done in the ARS system.



If you have never used your HSEN administrative account, you must first log into your workstation with that account to authenticate yourself on the domain. If not, your administrative account will not allow access to your administrative functions in WebStar. When complete, log off and log back in with your regular HSEN user account.

Reminder: Temporary passwords expire within 72 hours. If you have not logged in to your HSEN Administrative account or changed the password, you may not be able to log in until the password is reset.

Accessing WebStar

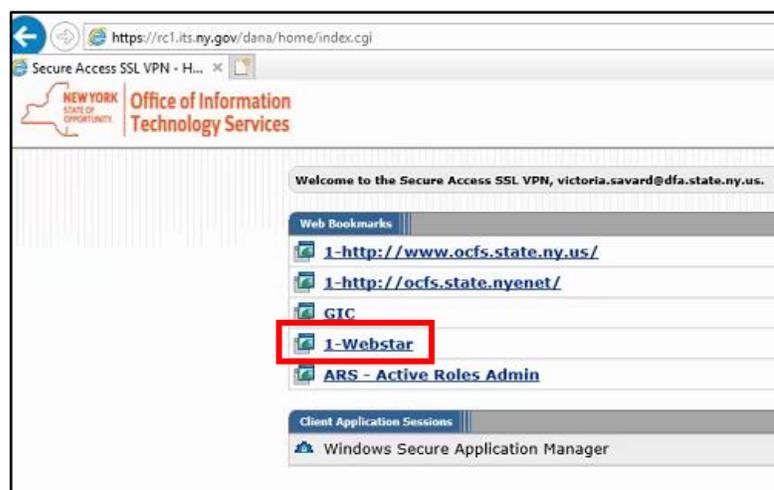
When logging on to WebStar, use your REGULAR account and password. DO NOT try to log on with your HSEN administrative account (HSEN\ADM(user ID))!

The ADM account is used to access administrative functions **within** WebStar, but you must use your regular HSEN account and password to log into the WebStar application itself.



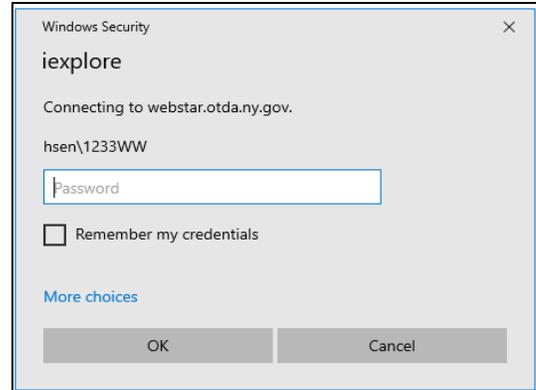
Note: WebStar will not acknowledge passwords that contain non-alphabetic characters (e.g., !, \$, #, %). If your password contains one of these characters, you will have to change your password to successfully access WebStar.

1. Log on to <https://rc1.its.ny.gov/hsen> to reach the NYS ITS landing page.
2. Click the **1-Webstar** link.



3. Use your **REGULAR** HSEN account and password (the ones you use to log into CONNECTIONS) to log in to WebStar.

This will bring you to the main WebStar page.



Reminder: you cannot unlock accounts or reset passwords in WebStar, even though it appears possible. These actions must now be done in ARS.

Creating a User Account

1. On the main WebStar page, **enter the password for your HSEN Administrative** account in the Active Directory Administration box.
2. Click the ***Click Here to Administer the Active Directory*** button.

WEBSTAR Office 365 [service now](#) [manual](#) [faq](#)

This site is not to be used for users that have been moved to the SVC domain
Requests for password reset assistance, that go to the ITS Service Desk
are now being directed to use the new Password Self-Service system
<https://password.ny.gov/>

Before users can use the Password Self-Service system, they will need to register their account.

HSEN ADMINISTRATORS can still administer HSEN accounts
by logging into Active Directory Administration below

Your Id is location within Agency Liberty Resources (IMK)

Michelle Walker's Webstar Menu

ATTENTION: For users and/or agencies that have not been migrated over to Office 365, please
contact NYSeMail to place a Service Request in regards to your mailbox handling.

[View latest Webstar/NewStar Updates](#)
[Common NewStar Documentation](#)

Your Active Directory Employer is []
Your HSEN ID [1233WW] is located in the Active Directory at:
All Users and Computers
Agencies
Liberty Resources (IMK)
Fulton 1850 County Route 57
Fulton 1850 County Route 57 Users

Your user account [1233WW] is a member of the following 11 groups

- CONX Voluntaries
- Fulton 1850 County Route 57 Conns
- Fulton 1850 County Route 57 Users
- LIBERTY-USERS
- Proxy Full New

You are permitted to perform the activities listed below:

Administer 3 APPLICATION Access Add/Update/Remove

Please enter your password for your regular account

APPLICATION Access Administration

Active Directory Administration
Webstar will use your ADM account [1233WW] for AD administration
If you encounter any problems, please contact the help Desk

[Click Here for HELP WITH WEBSTAR](#)

Select one administrative unit from the list below

- Liberty Resources LSAs
- Liberty Resources SOs
- Liberty Resources WOs

Please enter your password for your ADM account:

Click Here to Administer the Active Directory

You are currently connected to domain controller [DCS179PW5HSENDC] located at site [CNSE] in domain [HSEN].

Click Here to Choose a Different Site/DC

NOTE:
Changing your Site/DC is an advanced
feature and should only be used by
advanced users.

Your password will expire in 37 day(s) on 3/1/2020.
Your password for your ADM account will expire in 37 day(s) on 3/1/2020.

- On the Active Directory ADMINISTRATION Menu page, click the **Administer USER/Mailbox** button.

WEBSTAR HSEN Active Directory ADMINISTRATION Menu

[Click Here to OPEN WINDOW of NEW Standard USER Reports](#)
[Click Here to OPEN WINDOW of NEW Standard COMPUTER Reports](#)

You Are Permitted to Do the Activities Listed Below:

Administrator Designed Reports	HSEN Reports
Search HSEN	HSEN Inquiries
ADM Account Administration	ADM Account Administration
User Account/Mailbox Administration Create, Update & Delete	Administer USER/Mailbox
Workstation/Laptop Administration Create, Update & Delete	Administer Workstation/Laptop Account
SERVERS Only Administration Create, Update, Delete	Administer SERVER Account
Dial-In Access Menu Mountain Lake Childrens Residence (M48)	Dial-In Access
Standardize WEBSTAR Values for Job Titles, Departments, Offices	Mountain Lake Childrens Residence (M48) Values Menu *Help
Groups Administration Create & Update	Administer GROUPS

- On the User Accounts Menu page, click the **CREATE HSEN/Mailbox User** button.

nyseWEBSTAR HSEN Administer User Accounts Menu

Authority based upon ADMCT3083's membership in:
Mountain Lake Childrens Residence

HSEN Inquiries HSEN Inquiries
HSEN Reports HSEN Reports

TO RESET User Password Enter UserID <input style="width: 100px;" type="text"/>	<input type="button" value="RESET HSEN User Password"/> Help
UNLOCK HSEN User Account <input style="width: 100px;" type="text"/> Bulk Unlock Accounts	<input type="button" value="UNLOCK USER ACCOUNT"/> Help <input type="button" value="UNLOCK ACCOUNTS"/> Help
DISABLE HSEN User Account <input style="width: 100px;" type="text"/> REENABLE HSEN User Account <input style="width: 100px;" type="text"/>	<input type="button" value="DISABLE User Account"/> Help <input type="button" value="REENABLE User Account"/> Help
CREATE HSEN User & Mailbox Account	<input type="button" value="CREATE HSEN/Mailbox User"/> Help
MANAGE ACCOUNT HSEN User Attributes and Mail Object	<input type="button" value="UPDATE HSEN/Mailbox User"/> <input type="checkbox"/> Check Here to see ALL Possible Attributes On Next Page Help
PROXY/ZSCALER Settings for HSEN Users	<input type="button" value="Manage Proxy/ZScaler HSEN Settings"/>
DEPROVISIONING HSEN Mailbox	<input type="button" value="DEPROVISION HSEN/Mailbox Object"/>
DELETE User & Mailbox Account	<input type="button" value="DELETE HSEN/Mailbox User"/> Help
To UPDATE Specific Attribute enter UserID <input style="width: 100px;" type="text"/>	<input type="button" value="UPDATE Specific Attribute"/> Help

5. Enter the user's First Name, Initial (if known) and Last Name.
6. Select the appropriate Organizational Unit (agency location). For some agencies, the only OU will already be indicated.
7. In the Create HSEN/Mailbox Object box, your selection will depend on whether you wish to create a state email address for the user or to use an existing agency email address.

- Select the radio button for “**Mailbox & HSEN Account**” if you wish to create an account and a state email address (“@dfa.state.ny.us”) for the user.

Often, however, voluntary agency workers for whom a CONNECTIONS account is being set up, already have an existing email account at their agency. Rather than create an additional state email address, users can be set up as a “Custom Recipient” – meaning their existing agency email address can be associated with their regular (CONNECTIONS) user account and so that the worker doesn’t have two different email addresses to check for incoming messages.

Contact information for workers state email addresses as well as those set up as Custom Recipients is viewable in the statewide directory known as the Global Address List (GAL), available to all state and district workers.

- If you wish to use an existing agency email address for this user, select the radio button for, “**HSEN and Custom Recipient**” and enter the user’s agency email address (e.g., JBrown@abbotthouse.net)

8. Click the **Submit** button.

9. On the resulting page, complete the **Basic Information** for the user:

- Address
- Job Title
- Department (if any)
- Office (if agency has more than one)

This information will appear in the Global Address List (GAL). Once the account is created, any updates to this information must be made in ARS, not WebStar.

10. Enter the user's Office Phone Number. Do not enter additional phone numbers (Fax, Mobile) unless you wish these to display in the GAL.

11. Click the **Create a nyseWEBSTAR HSEN Account for** button to create the account.

12. Select **“New User of this System! No Existing Userid (Generate an ID)”** to generate a new ID number.

13. Click the **SUBMIT for CREATE** button.

A confirmation page will display, showing the temporary password and a new account number.

THE TEMPORARY PASSWORD WILL EXPIRE IN 72 HOURS.

PRINT THIS PAGE so you can pass this information on to the user.

2/12/2020 3:30:45 PM

HSEN Account & NYSeMail Creation Results

Creating HSEN/TZ9095 @ Lake Placid 50 Riverside Dr. Users
Mountain Lake Childrens Residence/M48

Creating User for Mountain Lake Childrens Residence (M48)
Results of Setting Password Value for HSEN (DCS179PW5HSENDC)/TZ9095 are listed below:

HSEN/TZ9095 Password Updated: Nonloser35\$

Created Mailbox on 2/12/2020 @ 3:30:46 PM by ADMCT3083

DisplayName will be: Pealer, Erica (DFA)

Region 4
Users Address Book will be DFA4 (Albany & Long Island Region)

Account HSEN/TZ9095 Created for Erica Pealer!

Account Added to Group 'Lake Placid 50 Riverside Dr. Users'
Found 'Proxy Blocked New' group.
Account Added to 'Proxy Blocked New' Group

Will Create a Home Directory for TZ9095 on Server HSEN-SMB

=====
Display Name: Pealer, Erica (DFA4-M48)

Results of Creating NYSeMail Mailbox for Erica Pealer (TZ9095) listed below:
NyseMail Email address is Erica.Pealer@dfa.state.ny.us

Action Audited Successfully

Please wait 5 minutes until the user's Home Directory becomes available

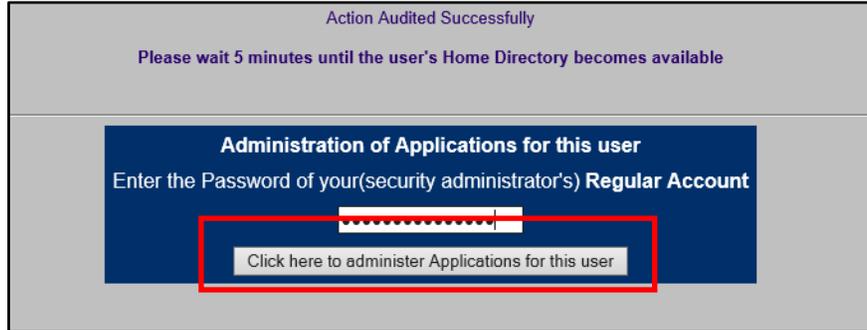
HINT: Since workers may not be able to reset a password within the 72-hour limit, some LSAs do not give the temporary password to their workers. Rather, after the account is created, they go into ARS and reset to a password that will not expire for 90 days. Users can then reset again, but without the time deadline of 72 hours.

NOTE: While this acknowledgement says the account has been created on the HSEN domain, it has actually been created on the SVC domain. When a domain is called for, users should sign in as "SVC\{UserID}".

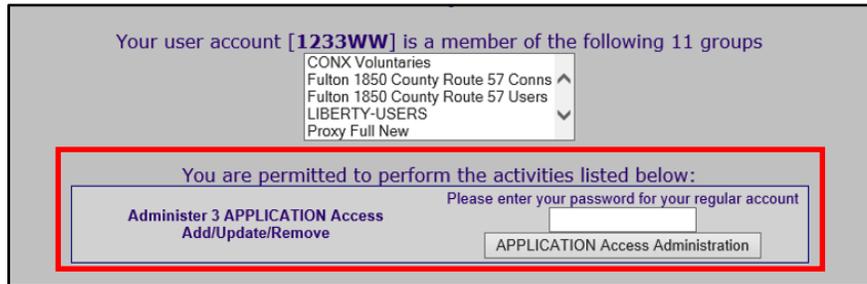
Adding CONNECTIONS Application Access

Creating the account in WebStar is only the first step in establishing user access to CONNECTIONS. Once the user account has been created, a second step, granting access to the CONNECTIONS application, must also be completed. This step is done in WebStar through the Application Access menu. An overnight batch is required to process the request, meaning the account will not display in CONNECTIONS until the following day.

1. Navigate to the Application menu either through the link on the page where you created the account or by logging in from the main WebStar menu to the Active Directory Administration page.



2. Log on by entering the password for your **REGULAR** HSEN account.

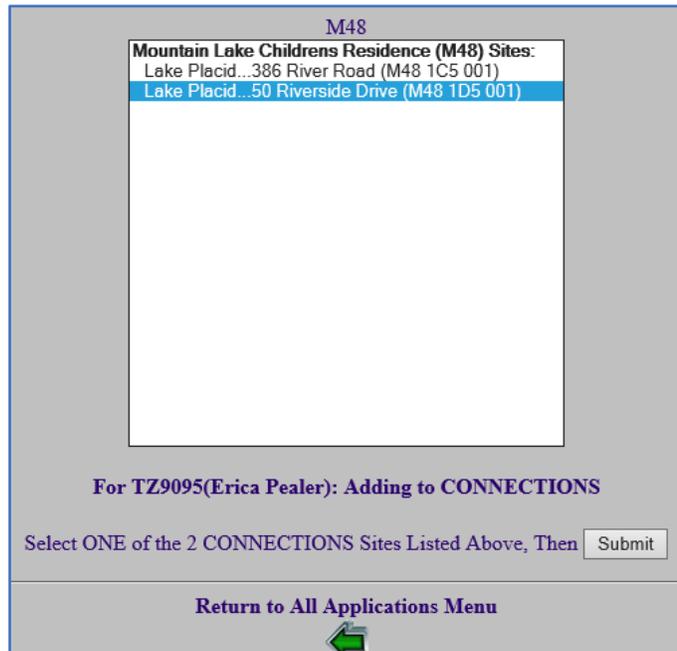


3. Click the **Click here to administer Applications for this User** button.

4. On the resulting window, click the **CONNECECTIONS Application** button.



5. Select the Organizational Unit to which this user will be assigned.



6. A page displays alerting you that the user has been successfully added to CONNECTIONS and that the process requires an overnight batch.

Mountain Lake Childrens Residence
Name=TZ9095
This Id is Stored in Active Directory @:
HSEN
Agencies
Mountain Lake Childrens Residence (M48)
Lake Placid 50 Riverside Dr.
Lake Placid 50 Riverside Dr. Users

Following Information for Site "ID5" Sent for "Adding to " to CONNECTIONS

NAME: Erica Pealer USERID: TZ9095
ADDRESS: 50 Riverside Dr. Lake Placid NY 12946
PHONE: +1 (518) 523-4300 Ext 119 TITLE: Admissions

Results of Adding to CONNECTIONS:

cmdtext: SELECT adspath, distinguishedName FROM 'LDAP://DCS179PW5HSEND/DC=HSEN' WHERE objectClass='Group' AND cn='Lake Placid 50 Riverside Dr. Conns'

hay group: Lake Placid 50 Riverside Dr. Conns

group:

Agency: Mountain Lake Childrens Residence
ConnGroupPath: LDAP://DCS179PW5HSEND/CN=Lake Placid 50 Riverside Dr. Conns,OU=Lake Placid 50 Riverside Dr. User Groups,OU=Lake Placid 50 Riverside Dr. Groups,OU=Lake Placid 50 Riverside Dr.,OU=Mountain Lake Childrens Residence (M48),OU=Agencies,OU=All Users and Computers,DC=HSEN

TZ9095 successfully added to Group 'Lake Placid 50 Riverside Dr. Conns'!

Wrote to Connections Trigger File Site ID5
User will be Activated in Connections Tonight
Connections Account not be Activated until tomorrow

Create TsNetInq OK

NYSEWEBSTAR for TERMINAL SERVICES Attributes
User will be Activated in Connections tonight
Connections Account not be Activated until tomorrow

Create TsNetInq OK

The new user will appear in CONNECTIONS the next day as a member of a temporary “Conversion Unit”, (typically named N01). There are additional steps that must be completed in CONNECTIONS to ready the account for use, which must be done by the agency’s CONNECTIONS Security Coordinator.

See the Tip Sheet **Adding a User to CONNECTIONS**, (Appendix A) for the specific steps necessary in CONNECTIONS.

The ARS (Active Roles Administration) Application

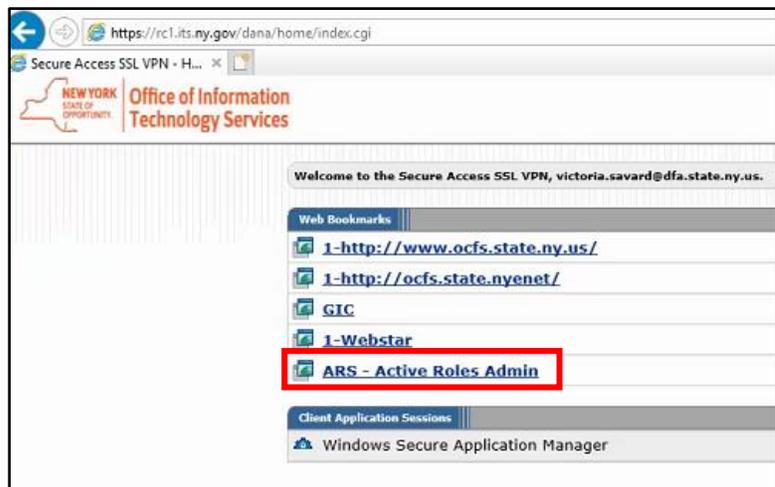
ARS is a web-based interface with the Active Directory. This new system will eventually replace WebStar completely. Tasks that were previously done in WebStar (resetting passwords, provisioning and deprovisioning accounts, etc.) have been transitioning to ARS. **Currently, WebStar is only to be used to create new accounts and mailboxes and to grant CONNECTIONS application access. ALL OTHER ACCOUNT RELATED ACTIVITIES MUST BE DONE IN ARS.**



Note: Before logging into ARS, you should first close any open windows WebStar related windows.

Accessing ARS

1. Navigate to the SSL-VPN landing page at <https://rc1.its.ny.gov/svc>.
2. Click on the **ARS – Active Roles Admin** link.



3. If you get this certificate warning, click “More information”, then “Go on to the Webpage”.

This site is not secure

This might mean that someone’s trying to fool you or steal any info you send to the server. You should close this site immediately.

[Close this tab](#)

[More information](#)

Your PC doesn’t trust this website’s security certificate.

Error Code: DLG_FLAGS_INVALID_CA

[Go on to the webpage \(not recommended\)](#)

For this warning, click the **Continue** button.



4. As your Username, enter your **SVC** administrative account – e.g., **SVC\ADM_(firstinitial)(lastname)** or **SVC\ADM(UserID)**
5. Enter the password for your **SVC** administrative account.

Note: Some users have experienced errors when logging in. If you run into issues, you may need to use a different browser such as Chrome instead of Internet Explorer or vice versa.

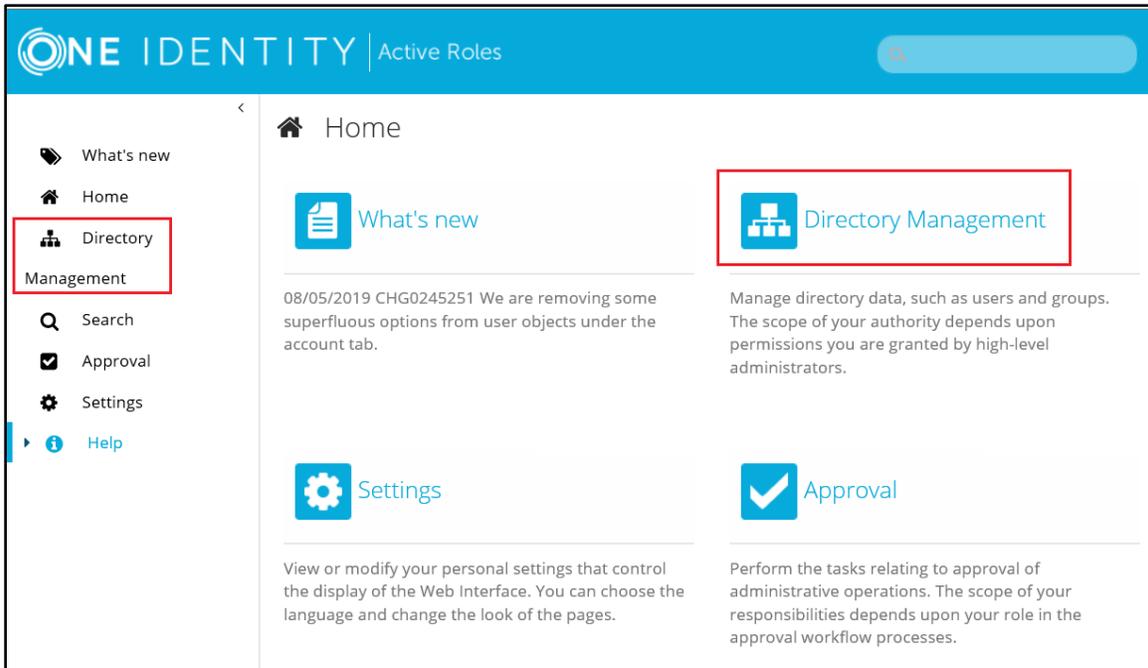
Navigating within ARS

To quickly locate a single user account for your agency, enter the user's name in the Search field in the Title Bar of the main page.



To locate a list of users or groups, use the following steps:

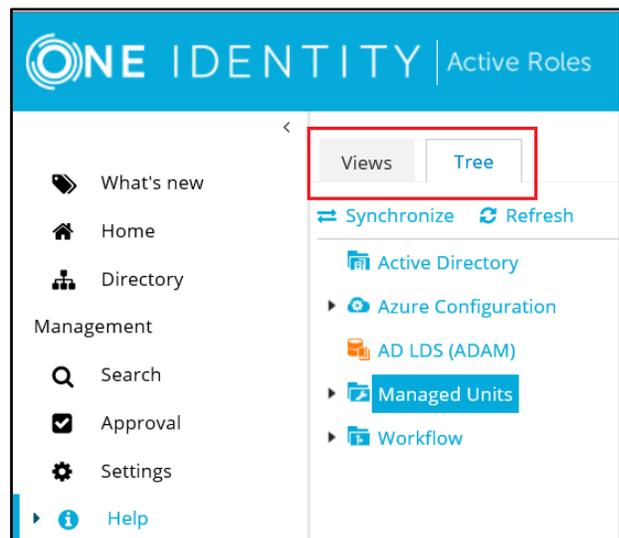
1. On the ARS home page, select one of the two **Directory Management** links.



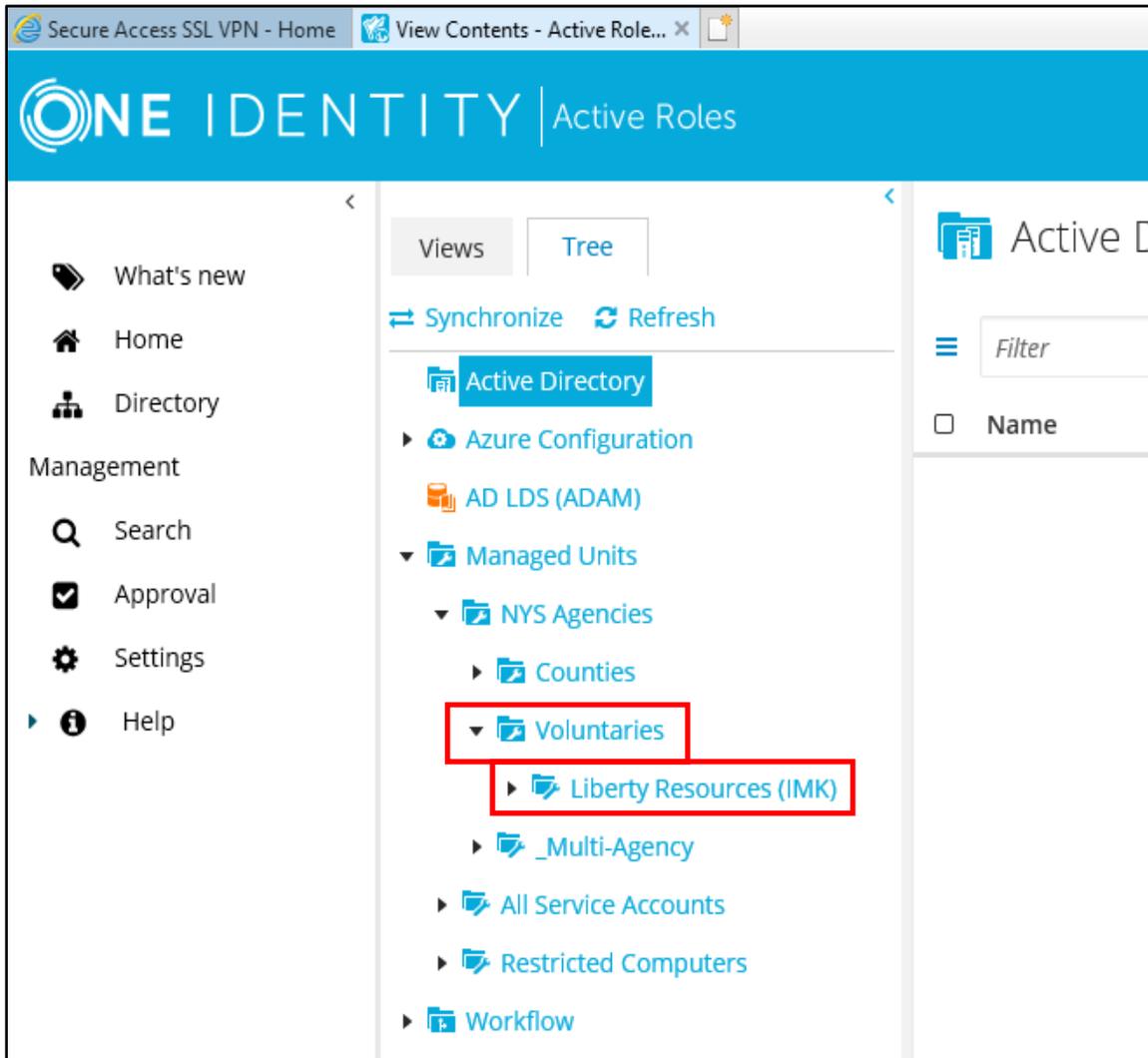
2. Click on the tabs to navigate from "Views" to "Tree".

3. Within the Tree view of Directory Management, select **Managed Units**.

The list of units which you can administer should appear to the right.



4. Select **Voluntaries**, then your **Agency** name.



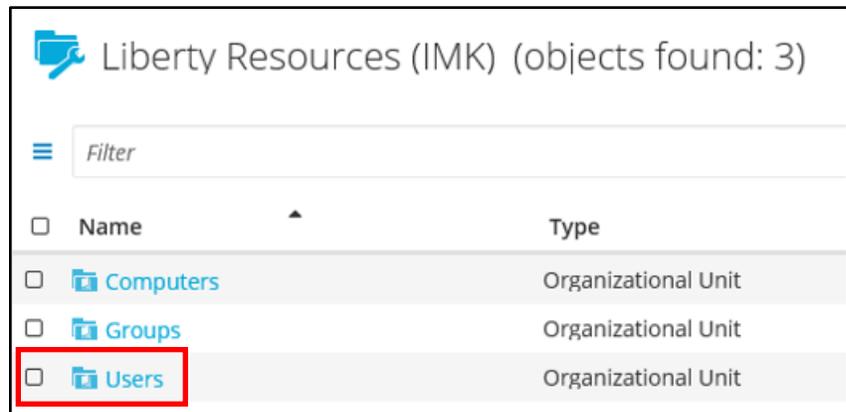
Note: The breadcrumbs which display at the top of the page - and may look like the image below (“Active Directory / svc.ny.gov / NYS Agencies”), will not function. An error will be displayed if trying to navigate using any of the breadcrumbs that start with “**Active Directory**”.

[Active Directory](#) / [svc.ny.gov](#) / [NYS Agencies](#)

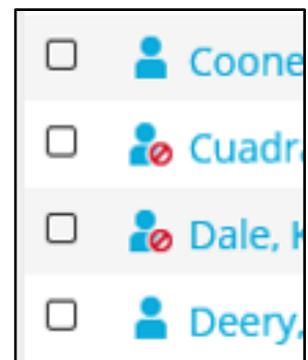
Breadcrumbs that begin with “**Managed Units**”, such as “Managed Units / NYS Agencies”, are functional at this time.

[Managed Units](#) / [NYS Agencies](#)

5. Click the **Users** link to display all the user accounts for your agency.



- Accounts that have been deprovisioned (disabled) will display with a red circle/slash on the icon by the person's name.
- An orange user icon means the account is locked.

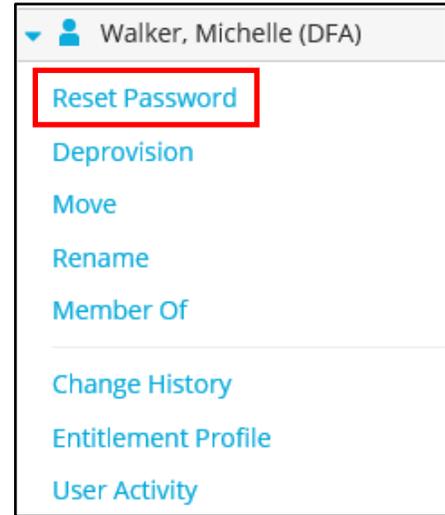


7. Select a user by clicking on their name.

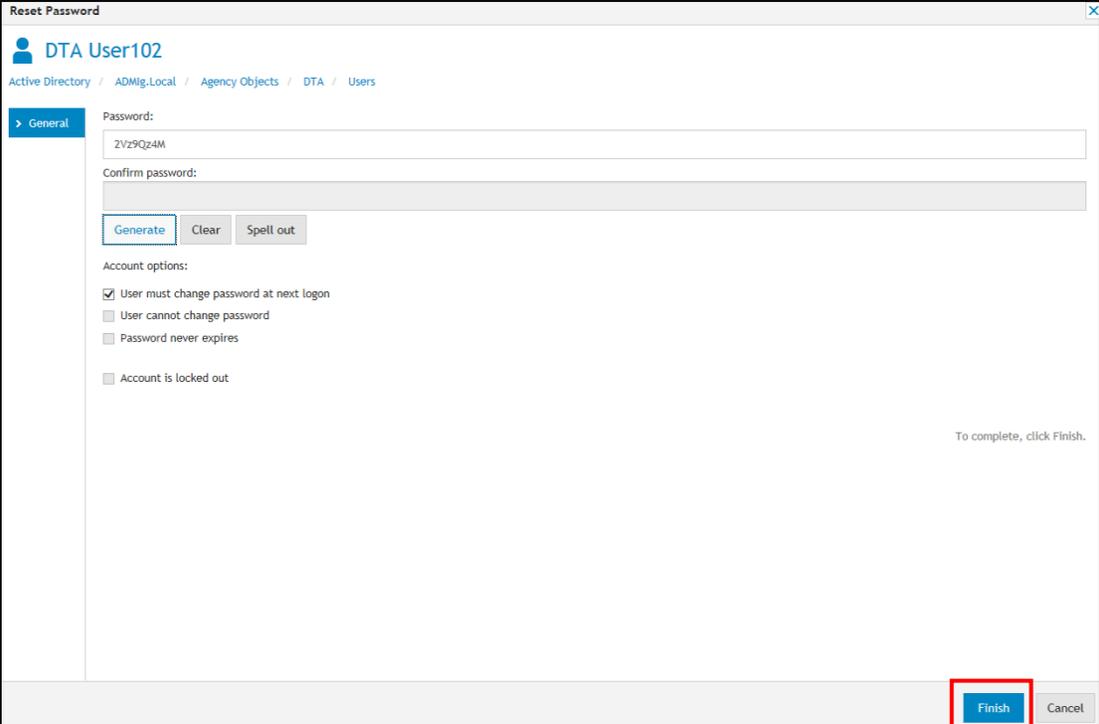
Password Resets in ARS

To reset a user's password, select the user and click the **Reset Password** link to the right.

1. Manually enter and confirm a password for the user or select the **Generate** button to allow ARS to randomly generate a complex password for the user.
2. Select **"User must change password at next logon"**.
 - **Do not select the "Password Never Expires" checkbox.** Per best security practices and ITS policy, passwords on regular accounts must be reset at least every 90 days.



3. Select **Finish** at the bottom of the window.

A screenshot of the 'Reset Password' dialog box. The title bar says 'Reset Password'. The user is identified as 'DTA User102'. The breadcrumb trail is 'Active Directory / ADMig.Local / Agency Objects / DTA / Users'. The 'General' tab is selected. The 'Password:' field contains '2Vz9Qz4M'. The 'Confirm password:' field is empty. There are buttons for 'Generate', 'Clear', and 'Spell out'. Under 'Account options', the checkbox 'User must change password at next logon' is checked. Other options are unchecked. At the bottom right, there are 'Finish' and 'Cancel' buttons. The 'Finish' button is highlighted with a red rectangular box.

4. ARS will display a confirmation at the top of the page if the password reset operation completed successfully.



Administrative Password Resets in ARS

If an Administrator's account is locked, there will be a check in the box "Account is locked out".

If the account's password has expired, the box to uncheck will not display, but the message "No Expiry (Must Change)" will display in the box under "Password Expires". This message means the Administrator must go to the <https://password.ny.gov> website to reset it. If they are unable to reset the password at password.ny.gov, they will need to call the Service Desk for assistance at **1-844-891-1786**.

General Properties

Baker, Carl ADM (DFA)

General
Address
Account
Telephones
Organization
Profile
Managed by
Picture
Published Certificates
Object
Request ID
Agency Specific

User logon name: ⓘ
admCT9192 @HSEN

* User logon name (pre-Windows 2000): ⓘ
SVC\ admCT9192

Agency Identifier:
 Account is locked out

Account expires:
 Never
 End of

Object
5/2/2020

Request ID
Password Expires:
7/1/2020, 3:43:51 PM
In 89 days

Workers Who Leave: Deprovisioning Accounts in ARS

When a worker leaves the agency either permanently or on an extended temporary leave (e.g., medical, maternity, family, etc.), their account should be "Deprovisioned" in ARS.

Deprovisioning encompasses the two account actions that were formerly known in WebStar as "Delete" and "Disable". ***These actions can no longer be done in WebStar. All account management must now be done in ARS.***

Deprovisioning an account in ARS will:

- disable the user account, removing access to CONNECTIONS and the Data Warehouse

- remove the user from any associated groups
- disable the user's email account if they have a state (“@dfa.state.ny.us”) email account. Custom Recipient email accounts are unaffected since they are based on the user's agency email address.
- If done for an LSA account, remove the LSA's ability to reach WebStar (since you log in with your regular account).

Email Management

The type of email account a user has will determine how it is affected by deprovisioning.

- Users with a state (“@dfa.state.ny.us”) email address will have their accounts go "stale" after 30 days of inactivity. the account is moved to the stale mailbox list. If the inactivity last 60 days, the mailbox will be deprovisioned and removed from the Global Address List (GAL). After 90 days of inactivity, the mailbox is deleted and is no longer recoverable. To prevent this, an "extended leave request" may be entered into the ITSM by your CONNECTIONS Implementation Team member (as VA users do not have access to the ITSM system).

The screenshot shows the 'Email Extended Leave' request form in the ITSM system. The form is titled 'Email Extended Leave' and includes a search bar at the top right. The main content area is divided into two columns. The left column contains a table with the following information:

Service Owner:	George Prevendoski (George.Prevendoski@its.ny.gov)
Phone:	+1 (518) 408-4706
Email:	George.Prevendoski@its.ny.gov
Service Level:	Mailbox will be placed on an Extended Leave status. This should occur within 24-48 hours of the request being made during normal business hours. Additional 24 hours may be required if mailbox has been de-provisioned.
Objective:	
In Scope Items:	This action will keep an users mailbox from being deprovisioned in the event of a long leave of absence
Out of Scope Items:	This assumes existing mailbox is present.
Availability:	Best Effort
Recovery Time:	Best Effort
Objective:	
Supporting Services Offered:	Individual incident resolution M # 7-5

The right column contains a 'Delivery Time: 2 Days' section with an 'Add to Wish List' button and an 'Order Now' button. Below this is a 'Required Information' section with a red warning box that says 'Short Description (Max 255 Characters)' and another red warning box that says 'Please select an Approver from the list of...'.

- Custom Recipient users, who receive email through an agency email address (e.g., Janet.Brown@cayugacenters.org) will not have their email accounts affected by the deprovisioning of their user account.
- RSA tokens are unaffected by the deprovisioning of a Custom Recipient email address, even though a state email address may be used as the primary user name when logging in to the SSL-VPN site.

Extended leave for the LSA Administrator

Ideally, if the person going on extended leave is the person with WebStar and ARS access, the agency would have a back-up LSA who can deprovision the necessary accounts and perform account creation or management duties in their absence. If there is no back-up, however, your CONNECTIONS Implementation Team Member can submit the request through ITSM to deprovision the LSA accounts.

An agency LSA cannot reprovision the LSA administrative accounts for another LSA at their agency, however. Reprovisioning must be done by ITS and will require a request done by your CONNECTIONS Implementation team member on behalf of the agency user through the ITSM system.

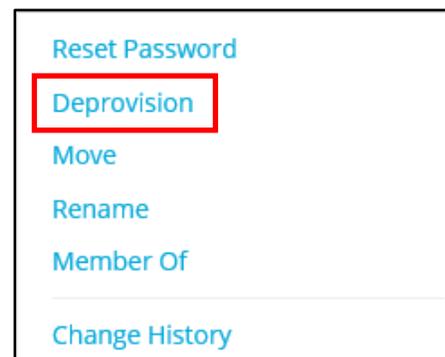
A reminder about RSA tokens:

- Token passwords expire yearly and must be reset to keep the token functional.
- If a worker is going to be on an extended temporary leave, they should check to see when their token expires and consider resetting it if it will expire during the course of their leave.
- Token passwords must be reset by the holder of the token; they cannot be reset by the LAN Administrator. Tokens and their passwords are not affected when an associated account is deprovisioned.

To deprovision an account:

1. Do a search or locate the user by following the steps above under “Navigating within ARS”.
2. Check the checkbox(s) for the user(s) you wish to deprovision. (More than one user account can be deprovisioned at a time).
3. Select the **Deprovision** link to the right.
4. Click the **Save** button.

Because of transitioning activities between WebStar and ARS, the list of users you see for your agency may include those end-dated in the past. These workers can again be deprovisioned in ARS.



Re-Enabling (Reprovisioning) an Account

When a user returns from an absence, their account can again be reprovisioned.

1. Do a search or follow the steps above under “Navigating within ARS” to locate the user.
2. Click the checkbox next to the user’s name and select the **Re-Enable with Groups** link to the right. This will add the user back to all the groups of which they were previously a member.
3. Click the **Save** button.

Note: If the LSA’s account was deprovisioned, the request to reprovision will need to be submitted in ITSM by your CONNECTIONS Implementation Team Member. Voluntary Agency LSAs cannot reprovision another LSA’s account.

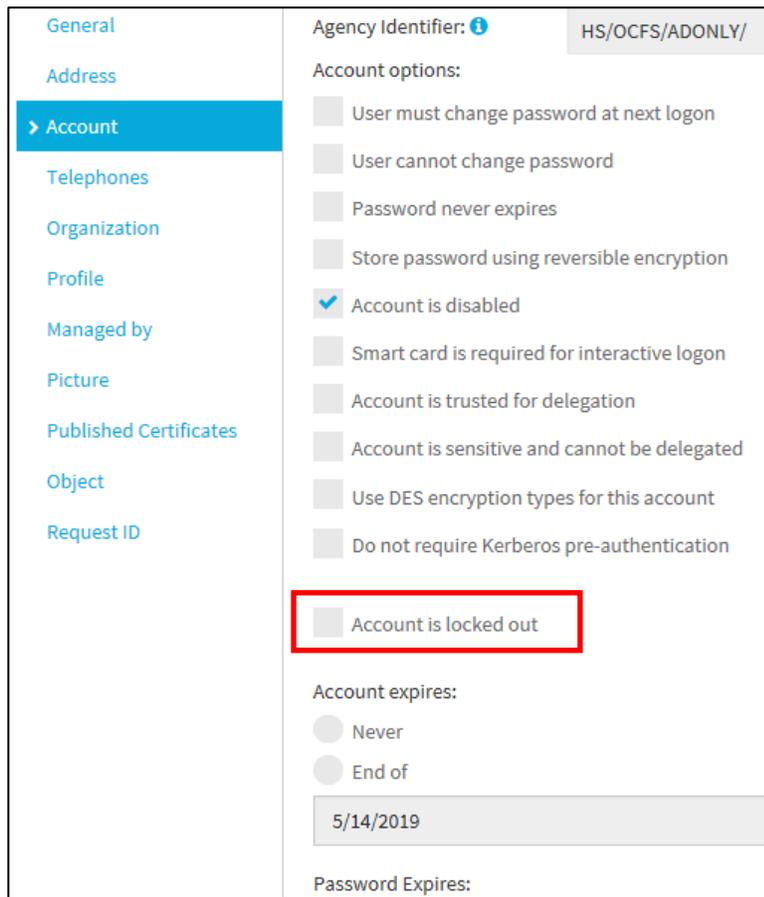
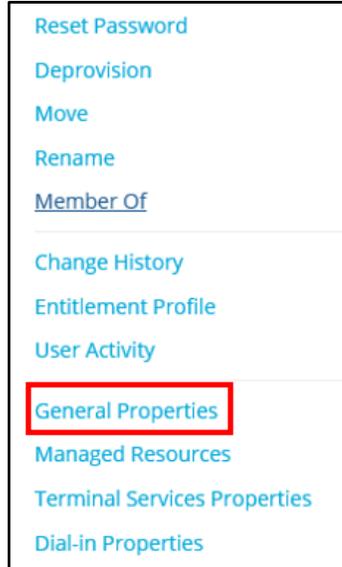
Unlocking an Account

If a user attempts to log in with the wrong password three (3) times, their account will lock. Administrators can unlock the account for the user in ARS.

 **User accounts can no longer be unlocked in WebStar.**

1. Do a search or follow the steps above under “Navigating within ARS” to locate the user.

2. Click the checkbox next to the user’s name and select the **General Properties** link to the right.



3. Click the **Account** link in the left navigation pane.

4. Uncheck the **Account is locked out** checkbox.

5. Click the **Save** button.

Managing Group Membership in ARS

Users are initially added to groups when their accounts are created in WebStar.



After the user account is created, any further group additions must be done in ARS.

In ARS, Voluntary Agency workers should be members of the following groups:

- **CONX Voluntaries**
- **(Site ID)-AllUsers** the Site ID is actually the Agency code – example Abbott House is P10
- **VLNTRY-CONX Voluntaries**
- **VLNTRY-Vol.shp.all.users**
- **VLNTRY-Site address**
- **Any specialty access like ReportNet or SSL-VPN access**

If the CONX Voluntaries group is missing:

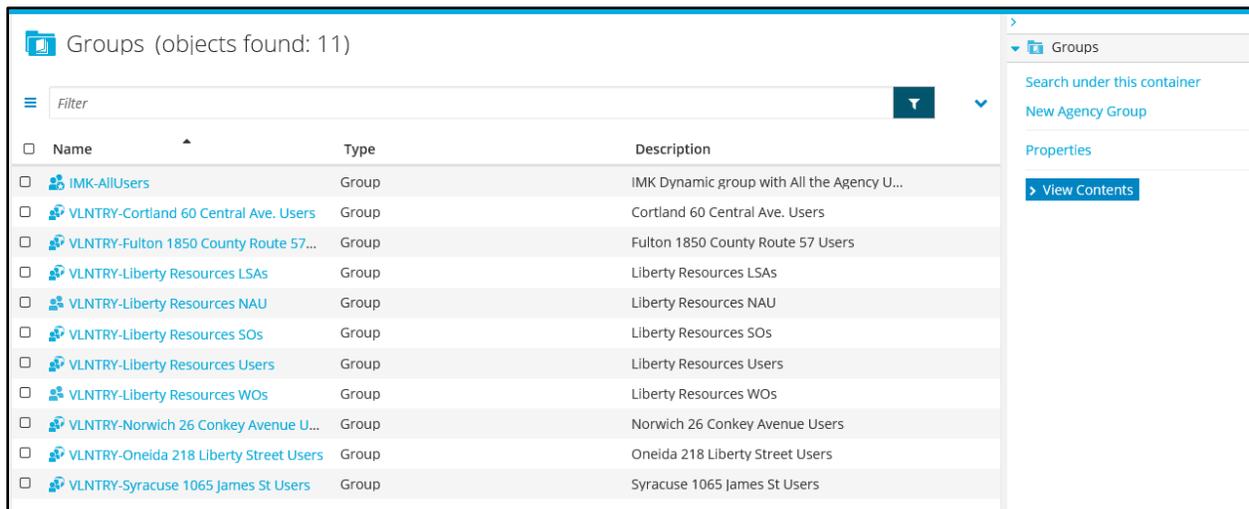
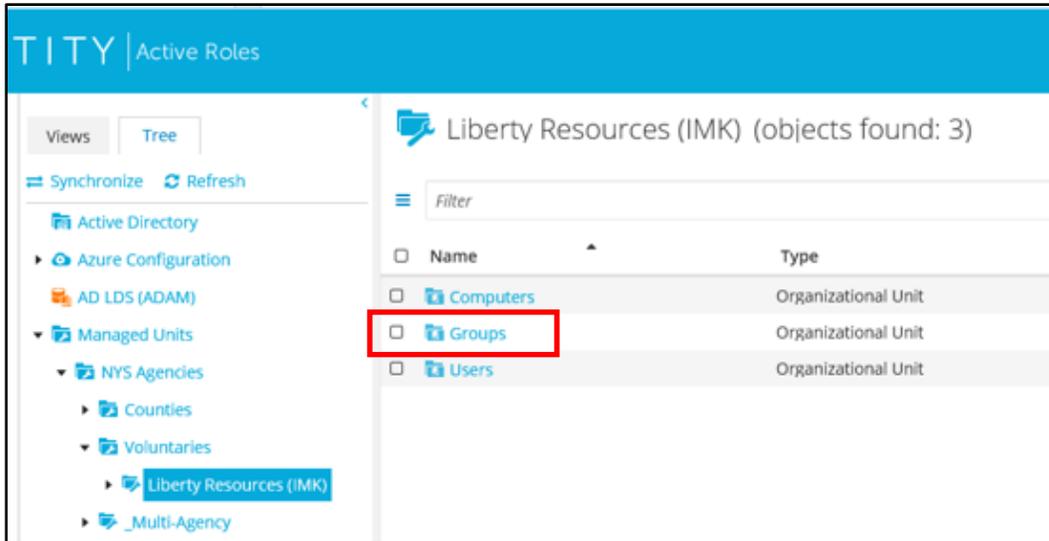
1. Click the **Add** button
2. Enter "CONX" in the Search field
3. Click Enter
4. Once propagated, select the option available and click the Save button

Sometimes the "CONX Voluntaries" option is not available when searching. This may indicate that the CONX Voluntaries group has not been added to the correct Organizational Unit (OU). If this is the case, try using "CONX Counties" instead.

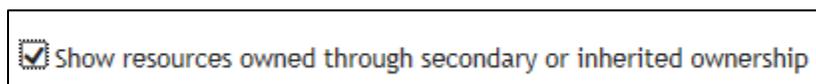
Users can be added to groups by either (1) locating the group and adding the user as a member or (2) locating a user and adding them to a group.

To locate a group:

1. From the main ARS page, select one of the two **Directory Management** links.
2. Click on the tabs to navigate from "Views" to "Tree".
3. Within the Tree view of Directory Management, select **Managed Units**.
4. Select **Voluntaries**, then your **Agency** name.
5. Click on the Groups link to display those for which you have been designated as **Manager**.



NOTE: If no groups are displayed, or if you are listed as a Secondary Owner, place a check mark in the box at the bottom of the screen labeled **“Show resources owned through secondary or inherited ownership”**.



There are two ways to view and modify the members of the groups:

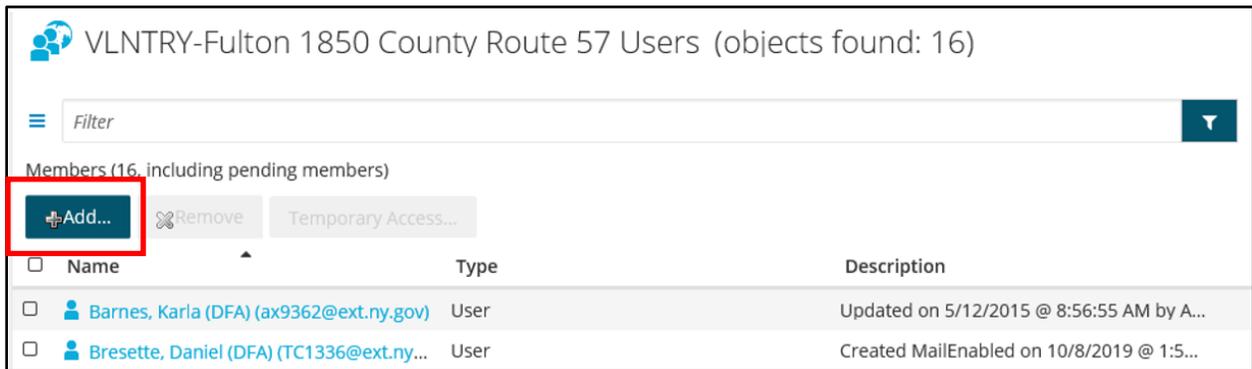
1. Clicking on the name of the group, or
2. Placing a check mark next to the name of the group and clicking on the **Members** link on the far-right side of the page.



After using either path, the membership list of the group should now display.

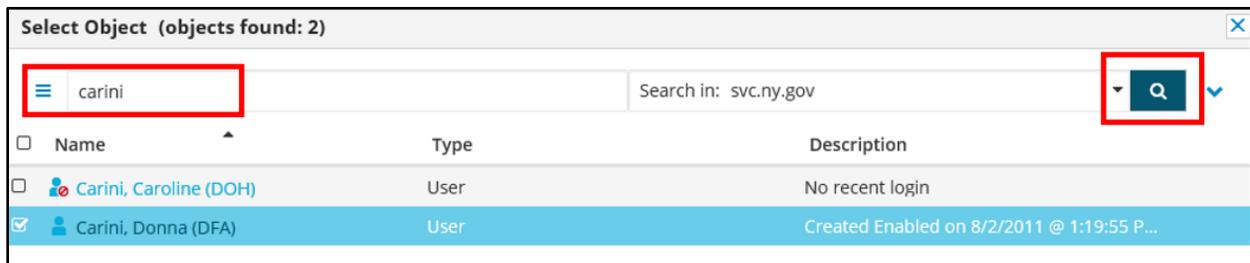
To add a user to the group:

1. After locating the group, click the **Add** button.



2. Search for the user to be added by either entering a portion of the user's name in the **Search** field or leaving the Search field blank to search for everything.

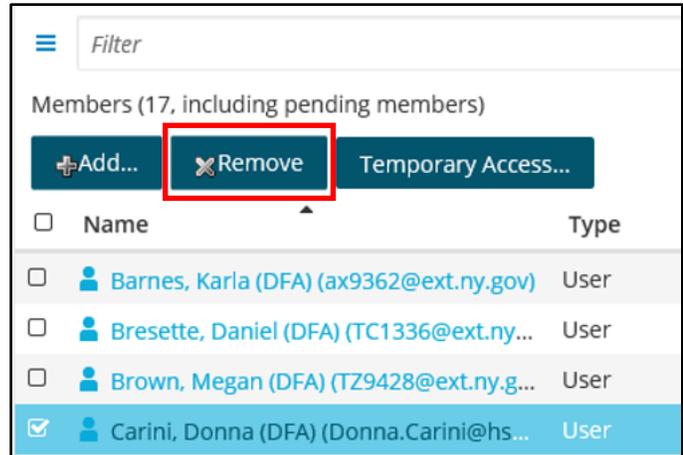
Click the Magnifying Glass button to conduct the search.



3. Check the checkbox next to the user's name.
4. Click the OK button in the lower right.

To remove a member from a group:

1. Navigate to the member list for the group.
2. Click the checkbox next to the user's name.
3. Click the Remove button.
4. Click the OK button.



The screenshot shows a user interface for managing group members. At the top, there is a 'Filter' input field. Below it, the text 'Members (17, including pending members)' is displayed. A row of three buttons is visible: '+Add...', 'Remove', and 'Temporary Access...'. The 'Remove' button is highlighted with a red rectangular box. Below the buttons is a table with columns for 'Name' and 'Type'. The table contains four rows of member information, each with a checkbox on the left. The first three rows have unchecked checkboxes, while the fourth row, for 'Carini, Donna (DFA) (Donna.Carini@hs...)', has a checked checkbox.

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	 Barnes, Karla (DFA) (ax9362@ext.ny.gov)	User
<input type="checkbox"/>	 Bresette, Daniel (DFA) (TC1336@ext.ny...)	User
<input type="checkbox"/>	 Brown, Megan (DFA) (TZ9428@ext.ny.g...)	User
<input checked="" type="checkbox"/>	 Carini, Donna (DFA) (Donna.Carini@hs...)	User

Troubleshooting Log on and Other Issues

There are several areas that have presented challenges to users attempting to access the SSL-VPN landing page, WebStar and ARS. Below are some of the problems encountered and potential solutions.

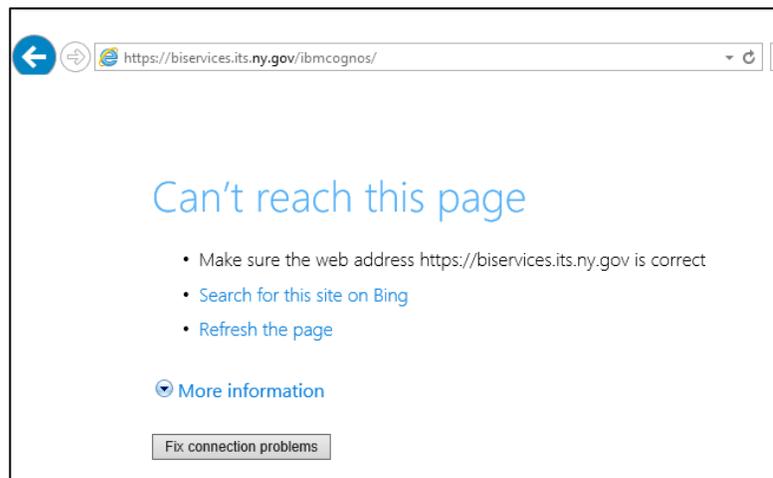


Note: You should not have multiple browser windows open when accessing either security application from the SSL-VPN landing page as this can cause corruptions. Please make sure that after using WebStar you close the application before accessing ARS as different credentials are required for each of these landing page links.

Pulse Secure

- In order to reach the SSL-VPN Landing page where the links to WebStar and ARS are located, the user's device must have the correct version of the Pulse Secure application installed.
- Pulse Secure works best with Internet Explorer as the browser.
- There are known issues with older version of Pulse Secure and Windows 10. If you repeatedly have access issues Your CONNECTIONS Implementation Team member can assist you in putting in a ticket through the ITSM system to have a newer version of Pulse Secure deployed.

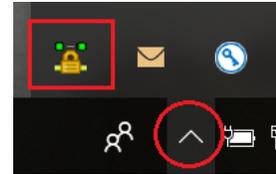
If you receive a "Page Cannot be Displayed" or "Can't Reach this Page" error when attempting to reach the NYS landing page, there is likely a problem with your Pulse Secure application.



Typically, installing the correct version of the software would be the responsibility of the Voluntary Agency's IT department as users do not generally have the administrative rights needed to install software on their own computer and may receive an error stating "You do not have the proper privileges to install the application".



To check for the Pulse Secure icon, check for the symbol in the lower right tray of your computer screen. You may have to click the carat (^) to display the icon.



- If the Pulse Client icon is greyed out and shows a status of “Disconnected”, the solution will be for the agency’s IT staff to uninstall all Pulse Secure related software and reinstall it.

It is a good idea to do a shutdown and manual restart after the un-install rather than a reboot. A reboot doesn’t always allow all the components to stop completely and may corrupt the re-install again.

Once Pulse Secure is successfully installed you should get a credential window login prompt when access WebStar or ARS.

- If you do not get a prompt for credentials and the Pulse Client is blue with a status of “Connected”, the agency has a firewall policy blocking webstar.otda.ny.gov.



If the firewall policy is the issue, the agency’s IT staff will need to create a rule to allow bi-directional traffic to the following IP addresses:

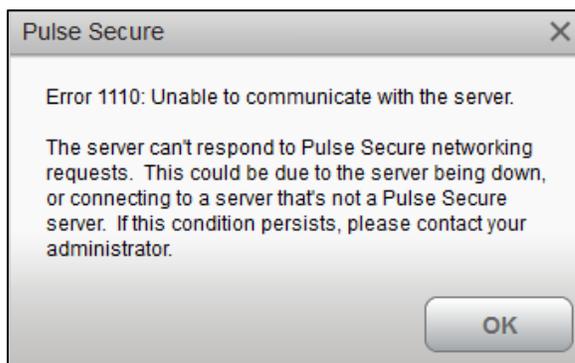
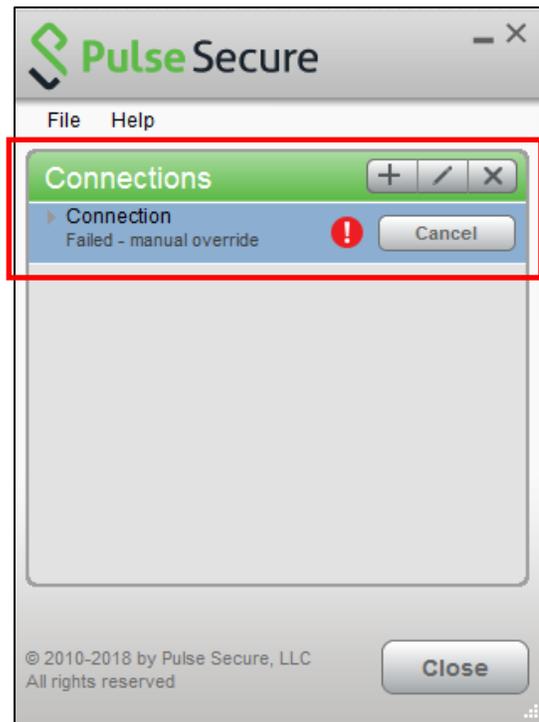
170.123.7.249

10.108.50.169

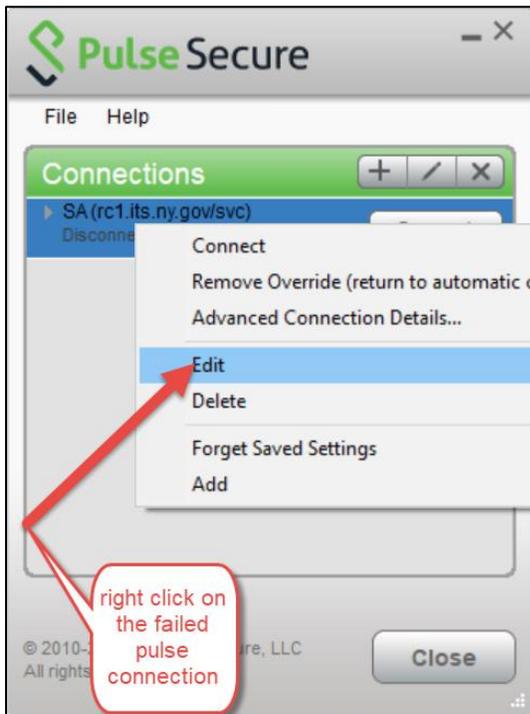
10.70.160.9

10.70.176.9

- Sometimes, the user’s CONNECTIONS profile corrupts during the installation of the Pulse Secure app, resulting in a “Connection Failed – manual override” error message.



To remedy this



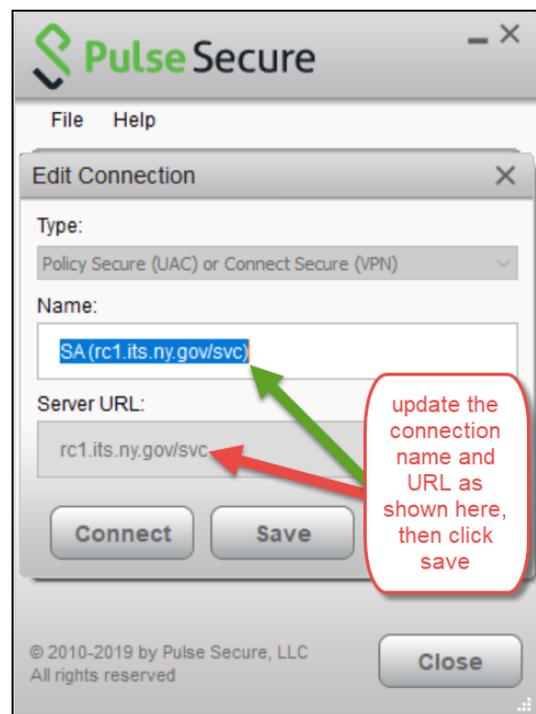
1. Right click on the failure message.

2. Select the Edit option.

3. In the Name field, enter **SA(rc1.its.ny.gov/svc)**.

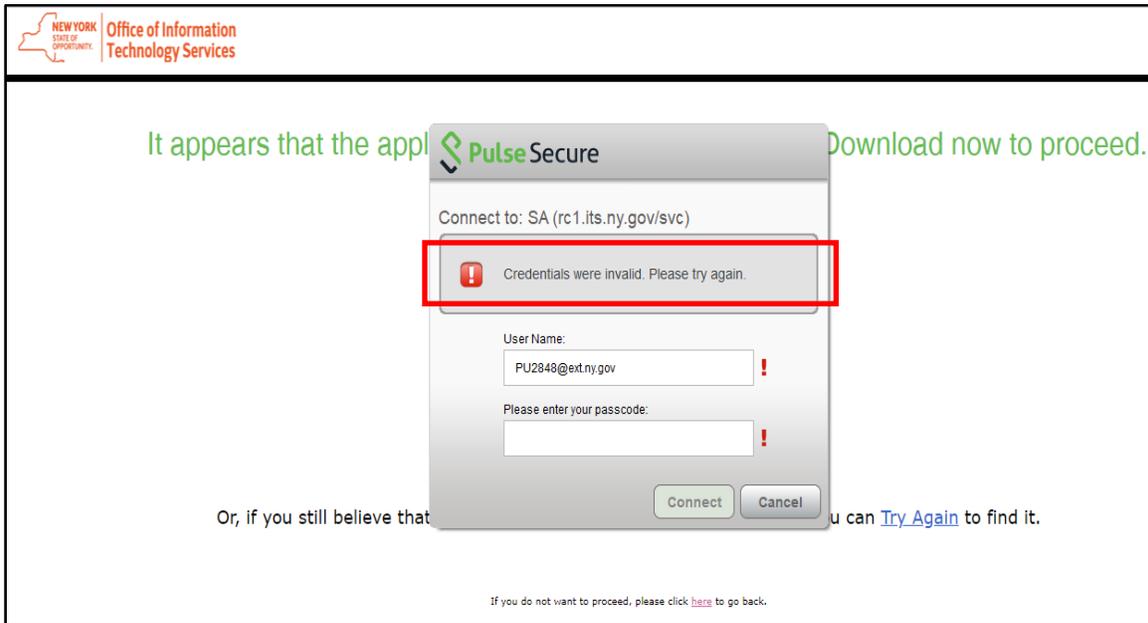
4. Update the Server URL to **rc1.its.ny.gov/svc**.

5. Click the Save button.



- If the user gets a prompt for credentials but receives a message that their credentials are invalid, this indicates that the host checker only runs via the web browser and the credentials cannot be validated.

Unless otherwise directed users should NOT login via the Pulse client but should use their web browser (Internet Explorer or Chrome) and login to <https://rc1.its.ny.gov/svc>.



You Are Not Allowed to Sign In Error

You are not allowed to sign in. Please contact your administrator.

This error message may have one of several causes:

- The user account has not been added as a member of the **cfs.grp.Connections.SSL.VPN** group
If this is the cause, a Service Request must be opened with the Helpdesk to add the user to this group.
- The user does not have a token, or the token may not be setup correctly.

Have the user login to <https://mytoken.ny.gov> with the email address they used when they set up their token (**NOT** their CONNECTIONS ID) and password. Verify that their security questions are set up correctly. See *Token instructions on pages 6-8 of this guide for more information.*

- The user's account may have been deprovisioned. This can happen to new users as the temporary password expires within 72 hours of it being issued.

The agency's LAN Administrator can check in ARS to see the user's account status. If it is the LAN Admin's account in question, a Service Request must be opened with the Helpdesk.

- The user is attempting to use a non-windows device such as a Mac or Android.

Reminder: Android devices should never be used to access CONNECTIONS as they do not allow a complete sign off. Hanging sessions prevent the user from logging in again.

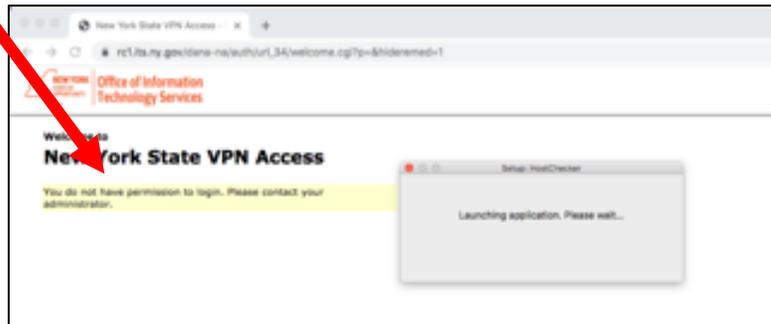
You Do Not Have Permission to Login Error

You do not have permission to login. Please contact your administrator.

This error can result when:

- The user may have entered an incorrect PIN or token code.

If so, verify and enter correct pin/token code.

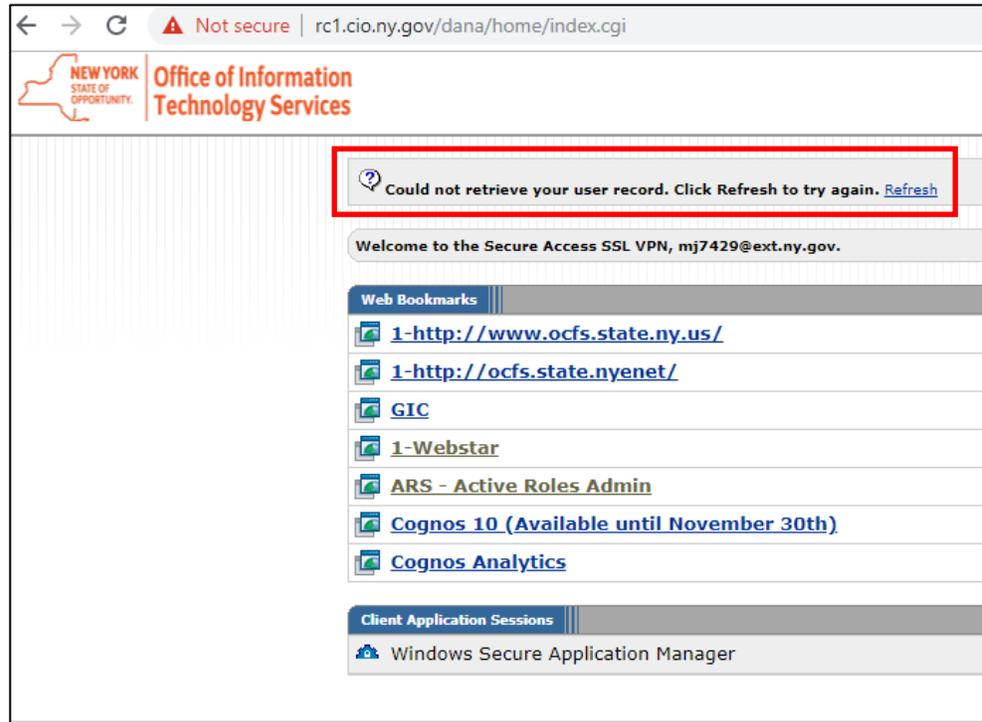


Could Not Retrieve Your User Record Error (WebStar and/or ARS links are greyed out)

There is no explanation for why these links grey out sometimes.

They may appear greyed out when using Chrome as a browser but not with Internet Explorer or vice versa.

Despite their appearance, the links still have an active connection and work.



Invalid Username or Password Error Message

Welcome to
New York State VPN Access

Invalid username or password. Please re-enter your user information.

Email Address: Please sign in with your RSA Token account(email address) to begin your secure session.
RSA token passcode: Soft Token users - enter Token code only
Hard Token users - enter 4-8 digit PIN & Token Code.

This occurs when the user is attempting to log in with the wrong credentials.

- The Email Address should be the email address used when you set up your token account. **This may not be the email address your regularly use.** The format may be something like the following:

[userid@ext.ny.gov](mailto:user@ext.ny.gov)

[userid@hsen.ny.gov](mailto:user@hsen.ny.gov)

[userid@dfa.state.ny.us](mailto:user@dfa.state.ny.us)

Firstname.Lastname@hsen.ny.gov

Firstname.lastname@dfa.state.ny.us

Firstname.Lastname@ext.ny.gov

- For the RSA token passcode,
 - If you are using a hard token, you must enter the PIN you created when you activated your token, followed by the token generated code (no spaces between).
 - Soft tokens only require entry of the generated code (no PIN).
- If you get a message that the token passcode is not correct, verify that you are using the correct pin to generate a token code. One of the flaws with a soft token is that even if your pin is not 1234 and you enter it, it will generate a token which will not validate against the RSA token database as a valid passcode.

HTTP Error 401.1 – Unauthorized Error Page

HTTP Error 401.1 - Unauthorized

You do not have permission to view this directory or page using the credentials that you supplied.

Most likely causes:

- The username supplied to IIS is invalid.
- The password supplied to IIS was not typed correctly.
- Incorrect credentials were cached by the browser.
- IIS could not verify the identity of the username and password provided.
- The resource is configured for Anonymous authentication, but the configured anonymous account either has an invalid password or was disabled.
- The server is configured to deny login privileges to the authenticating user or the group in which the user is a member.
- Invalid Kerberos configuration may be the cause if all of the following are true:
 - Integrated authentication was used.
 - the application pool identity is a custom account.
 - the server is a member of a domain.

Things you can try:

- Verify that the username and password are correct, and are not cached by the browser.
- Use a different username and password.
- If you are using a custom anonymous account, verify that the password has not expired.
- Verify that the authenticating user or the user's group, has not been denied login access to the server.
- Verify that the account was not locked out due to numerous failed login attempts.
- If you are using authentication and the server is a member of a domain, verify that you have configured the application pool identity using the utility SETSPN.exe, or changed the configuration so that NTLM is the favored authentication type.
- Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click [here](#).

Detailed Error Information:

Module	WindowsAuthenticationModule	Requested URL	https://webstar.otda.ny.gov:443/
Notification	AuthenticateRequest	Physical Path	C:\inetpub\wwwroot\WEBSTAR_2018
Handler	StaticFile	Logon Method	Not yet determined
Error Code	0xc000006d	Logon User	Not yet determined

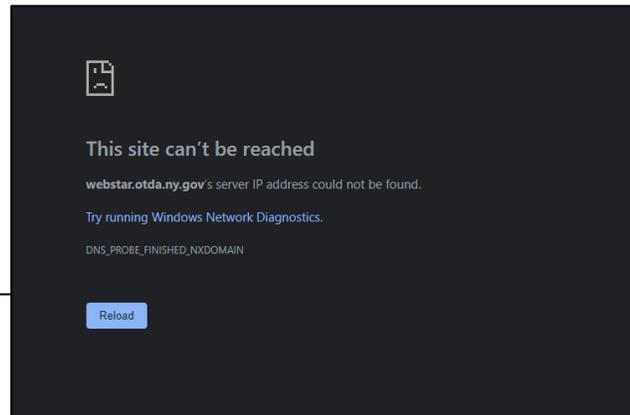
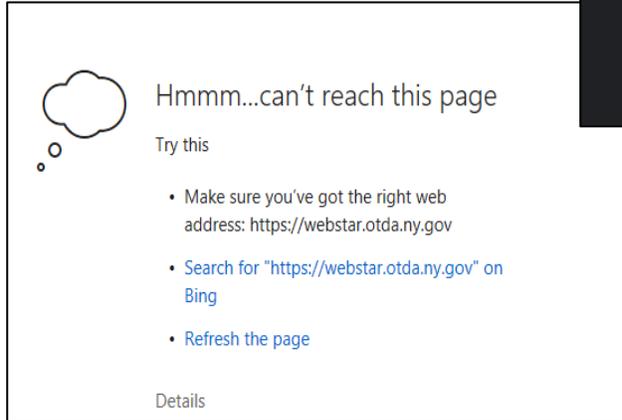
More Information:
This error occurs when either the username or password supplied to IIS is invalid, or when IIS cannot use the username and password to authenticate the user.

This error results when the user is attempting to log into Webstar.otda.ny.gov with the wrong format/credentials.

You must log into WebStar with your regular HSEN account (HSEN\userID) and the password you use to access CONNECTIONS. The HSEN administrative account is ONLY used within WebStar.

Site Can't be Reached or Can't Reach this Page

These are examples of Windows 10 based errors that display when the browser cannot resolve the IP address for the WebStar URL. When Windows is updated to version 1901 and higher, their version of the Pulse client gets broken - and so does access to WebStar.

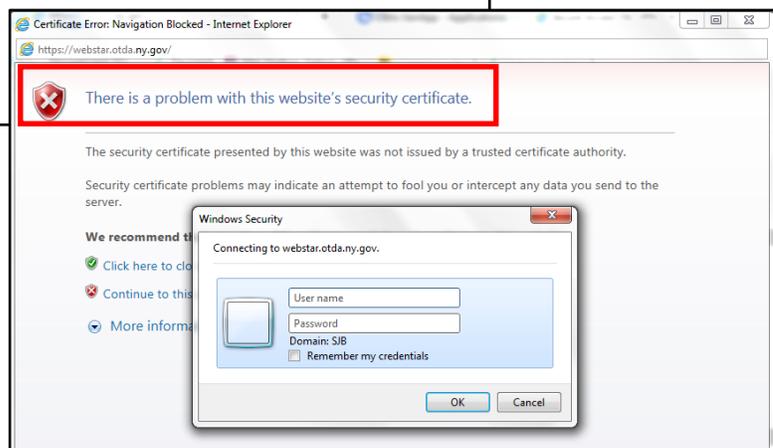
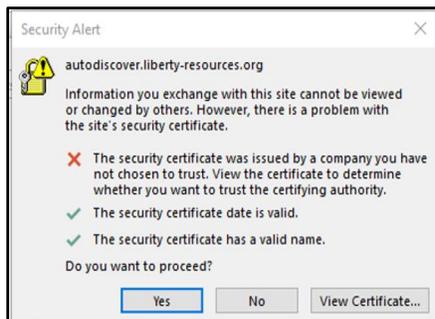


ITS has been moving the user off the old instance of the client and on to the new one to remedy this.

ITS is planning an update to the SSL-VPN software that will resolve this issue in the near future.

In the meantime, users should open a ticket with the Helpdesk and request that it be sent to the WebStar team.

This Site is Not Secure/Problem with Website's Security Certificate Error



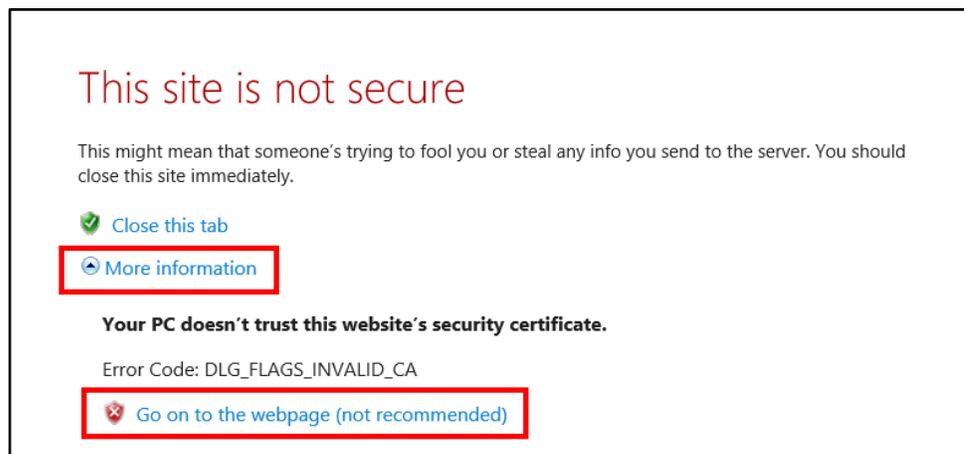
WebStar and ARS have a security certificate that was issued internally by NYS-ITS. This error results when the user's workstation is not able to read that certificate via SSL-VPN. **This is not actually a security risk.**

The IT department of a Voluntary agency can open an incident through the ITS Helpdesk to request the WebStar certificates and install them locally. If your agency has many pc's, the certificate will have to be deployed by group policy.

However, this error does not prevent a user from getting to and using WebStar or ARS.



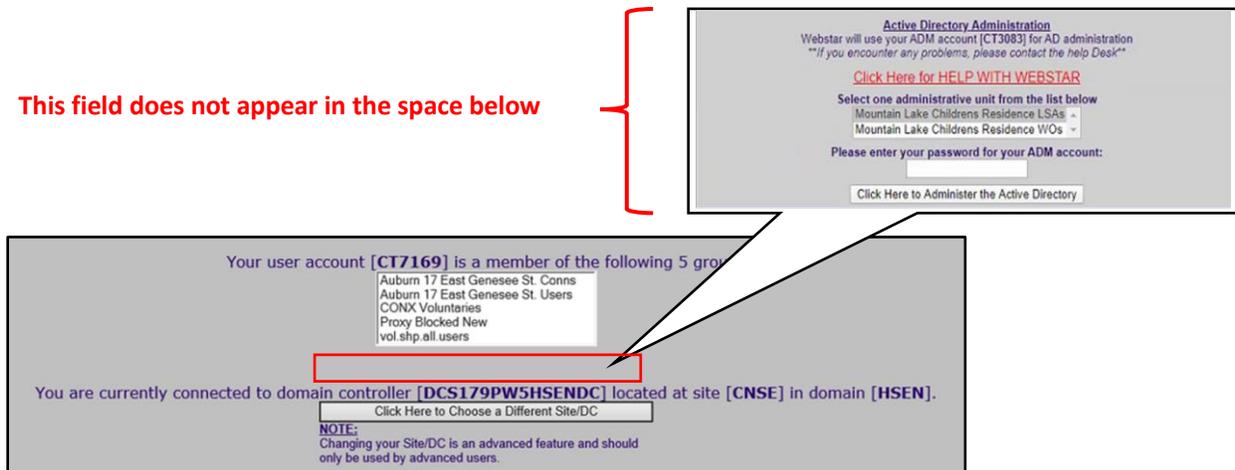
1. Click the **More Information** link.
2. Click the **Go on to the webpage** link.



The Active Directory Administration Fields Do Not Display in WebStar

If you can successfully reach the main WebStar page, but the Active Directory Administration log on fields do not display, there is a problem with your HSEN Administrative Account. It may have been deprovisioned, or not correctly formatted when it was set up.

This field does not appear in the space below



You will need to contact the Helpdesk open a Service Request (incident) to see if your account is still active and/or set up correctly.

You Do Not Have Local Security Administrator (LSA) Permissions (WebStar)



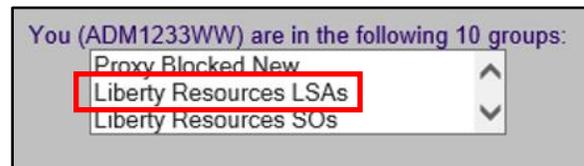
This error typically happens when a new LSA account is created and/or reprovisioned and the user has not been correctly added to the right WebStar LSA group(s).

Since this is an HSEN group specific to WebStar, it will not be reflected in the user's group memberships as shown in ARS.

You will need to open a Service Request (incident) with the Helpdesk to get this resolved.

Request that the Zone Team access whether or not user is in the correct LSA groups. If the Zone Team is unable to confirm this, request that the ticket be escalated to the WebStar group.

The correct group will be "Agency name (sometimes with a site address) LSAs"



WebStar Error 8007085a

This error occurs when your administrative (ADM) account password has expired and needs to be reset.



Unable to Re-access WebStar after Creating a New Account and being Knocked Out of the Application

Some users have experienced a problem of being knocked out of the WebStar application after successfully creating a new user account, but before being able to add CONNECTIONS application access for the user. They then are not able to immediately log back in to WebStar to complete the process.

If this occurs, try the following:

1. Log out of the NYS ITS browser session
2. Clear the browser cookies.
3. Exit the browser
4. Reopen the browser and try again.

If using Internet Explorer, the path is:

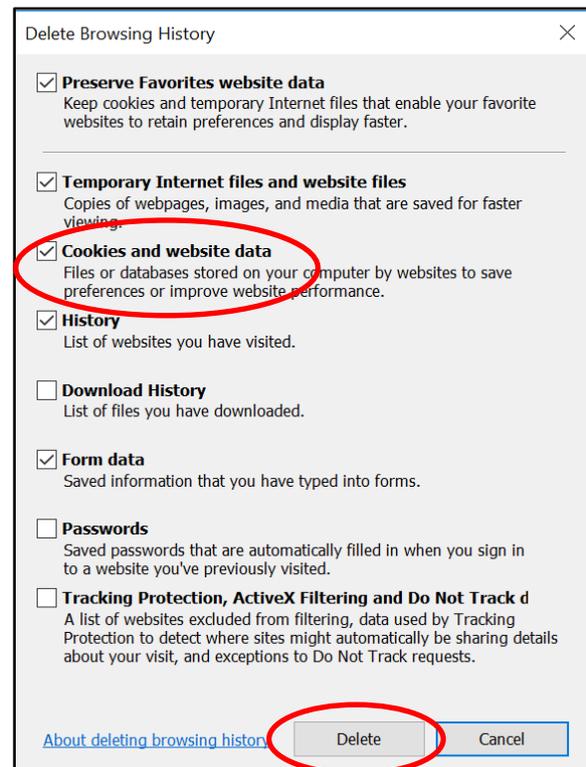
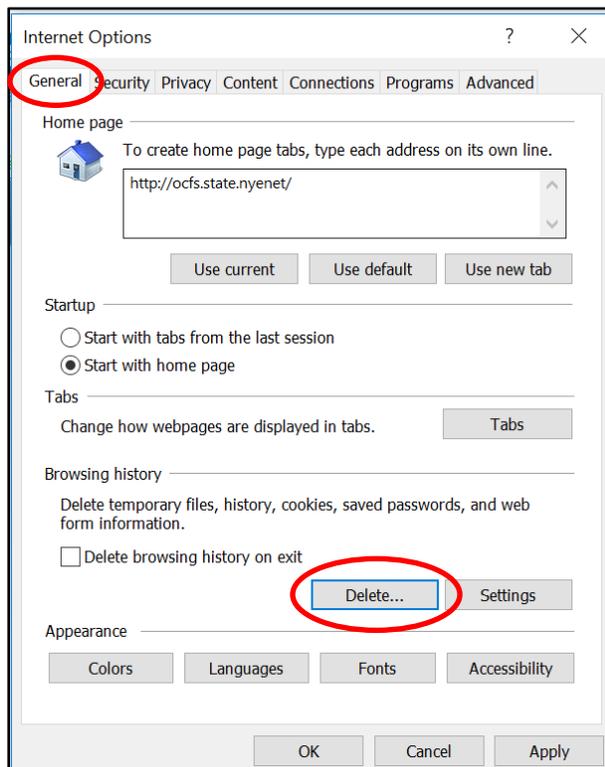
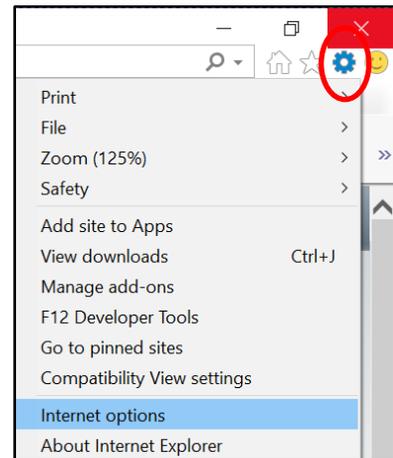
Settings > Internet Options >

General tab > Delete button >

Delete button >

Apply button >

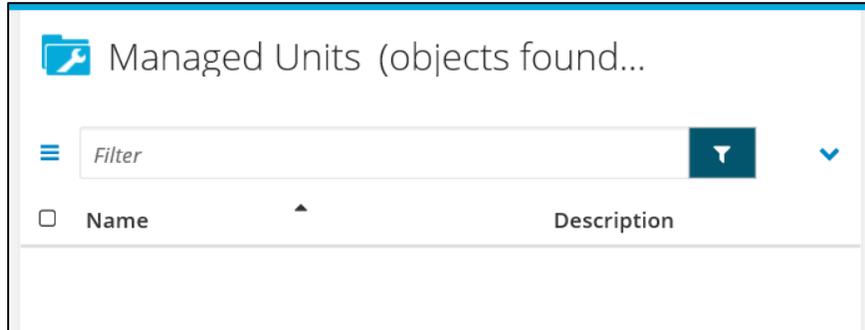
OK button



No Groups Display in ARS

If the SVC Special Access Account was not assigned to any Organizational Unit(s) when it was created, no groups will display for the agency in ARS.

Adding OU access must be requested by your CONNECTIONS Implementation Team member through ITSM.



Note to CONNECTIONS Team Members:

Changes to Administrative accounts need to be submitted via the ITSM Self Service Portal>Service Catalog>User Accounts and Access>Active Directory (AD) Privileged & Service Accounts.

- Service Type: **Account**
- Account Type: **Privileged Account**
- Request Type: **Change**
- Domain: **SVC**

Approval Group

i BUS Approvers OCFS

* Please select an Approver from the list of your Agency Authorized Approvers below.

i Peter Whitford (Peter.Whitford@ocfs.ny.gov) x

* Service Type

Account

* Account Type

Privileged Account (Used by individual users to administer systems)

* Request Type ?

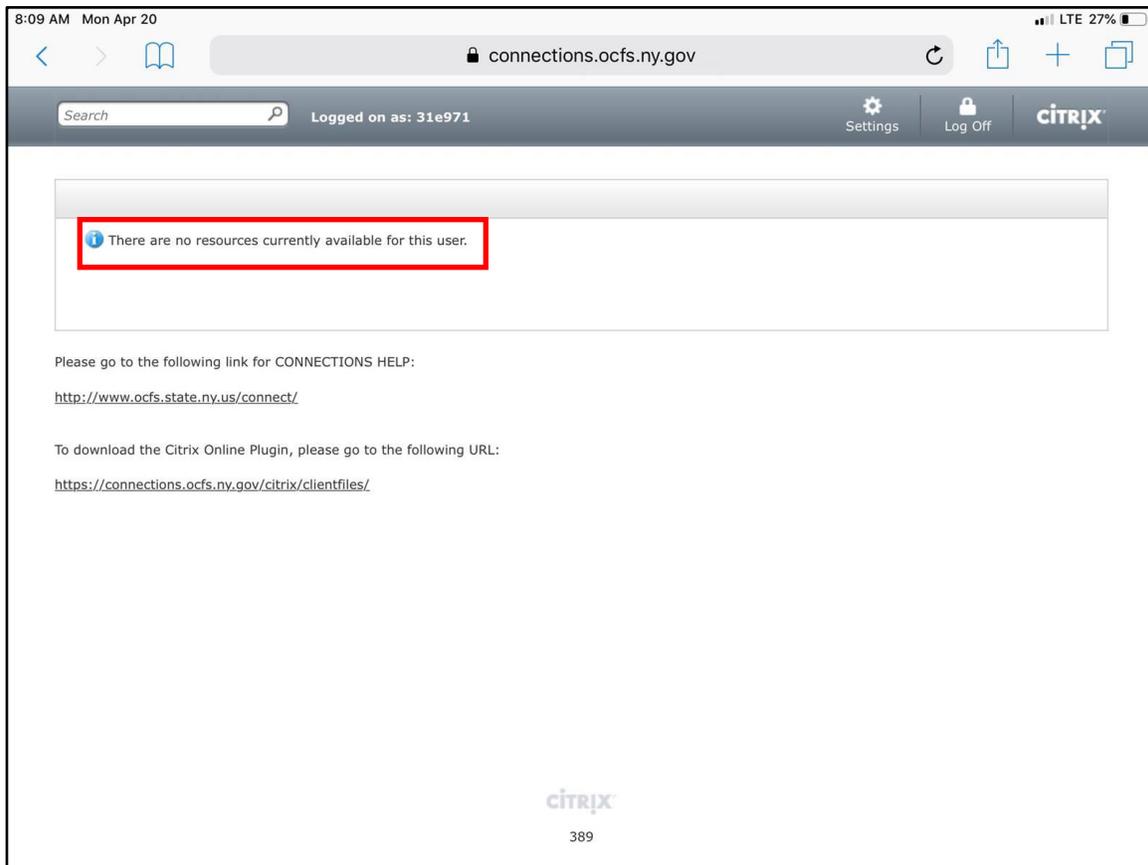
Change

* Domain

i SVC - svc.ny.gov x

There are No Resources Currently Available for This User

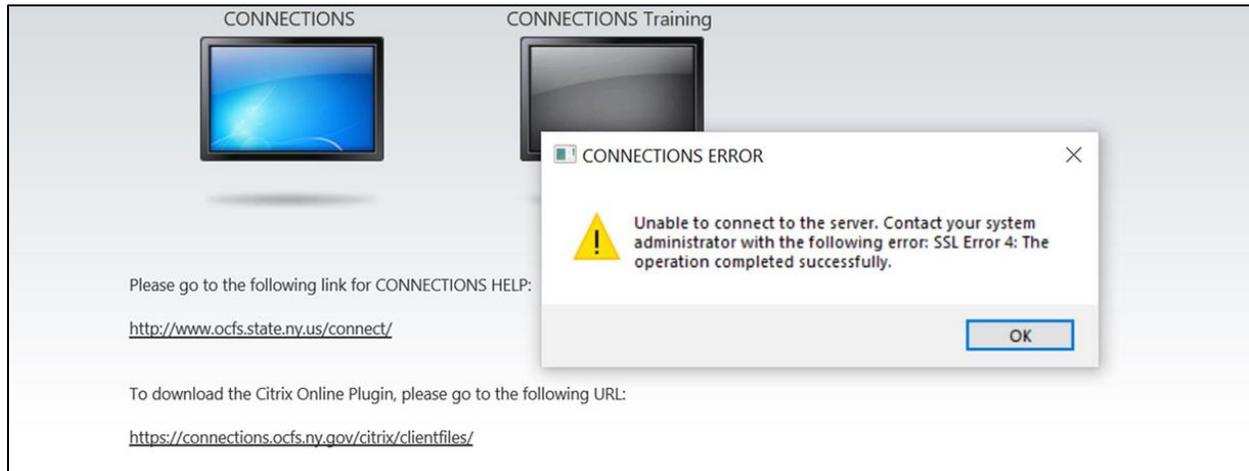
This error occurs when a user attempt to log into CONNECTIONS, but the user does not have the needed CONNECTIONS entitlements.



Users can also receive this message when the CONNECTIONS application is temporarily down. In this circumstance, they should be advised to try again later.

SSL Error 4

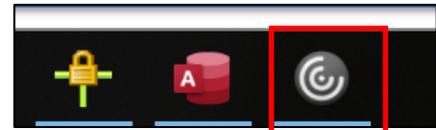
This error is encountered when the user attempts to log into CONNECTIONS.



This is a communication issue between the Citrix Client and the Citrix Gateway for which Citrix has not discovered a cause.

To remedy this:

1. Log out of CITRIX and exit completely (Make sure it's not running in the system tray as well.)



2. Delete browser cookies, making sure to always uncheck "Preserve Website Favorites Data"
3. Close the browser

If these steps do not resolve the issue, as a last resort, shut down the computer completely and turn back it back on. This may or may not resolve the problem.

If all the above steps do not work, uninstall the Citrix Receiver, reboot the computer, then re-install.

If this fails to resolve the problem, contact the ITS Enterprise Service Desk at 844-891-1786 or email them at FixIt@its.ny.gov for assistance.