

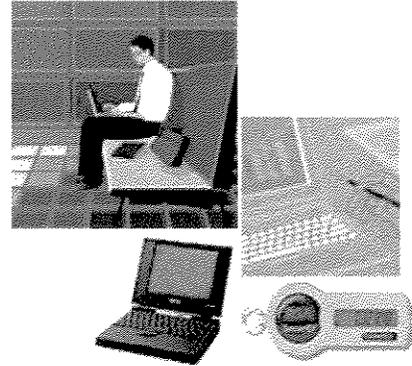
APPENDIX J

SECURE TOKENS INFORMATION

Virtual Private Network and Secure Tokens

ODJFS has created a secure Virtual Private Network (VPN) that allows personnel to use a secure token to log into the network whether you are at home, in an airport, or working remotely from another office.

Until now, ODJFS has used the Department of Administrative Services (DAS) dial-up program. If you currently have a DAS secure token, continue using it. As the DAS secure tokens reach their expiration date, they will be replaced with ODJFS secure tokens.



The differences between the DAS secure token and the ODJFS secure token are listed below.

DAS Tokens:

- Require dial-up only connections and a 56K modem
- Provide connectivity to the Mainframe only
- Require the user to supply a PC, such as a laptop.

ODJFS Tokens:

- Require an internet connection, Broadband or DSL
- Provide connectivity to the Mainframe, InnerWeb, P:\ Drive, R:\ Drive, and other shared drives
- Provide support from the Bureau of Network Support (BNS) to configure and support State-owned laptops. Users with a personal laptop or computer at home can request a secure token, however BNS does not support personal computers.
- Are part of a growing VPN network adding additional applications in the future.

Requesting VPN Access

VPN Requests
<ul style="list-style-type: none">▪ Requesting VPN Access for State Personnel▪ Requesting VPN Access for County Personnel▪ External Entity VPN Process<ul style="list-style-type: none">○ VPN Requests for External Entities Personnel

Secure Tokens
<ul style="list-style-type: none">▪ The Secure Token▪ Using the VPN to Log Into the ODJFS Network▪ Replacing an Expired Secure Token

Administering VPN

Manager Responsibilities
<ul style="list-style-type: none">▪ Removing VPN Access for Terminated Employees

VPN Problems
<ul style="list-style-type: none">▪ Reporting a Lost or Stolen Secure Token▪ Reporting a Lost or Stolen Laptop▪ Providing VPN Support

External Entity VPN Process

Before You Begin

MIS Managers must request VPN access for external entity personnel. If the request does not come from an MIS manager, the request will be delayed, and may be denied.

Requesting VPN Access for External Entity Personnel

Follow the instructions below to request VPN access for external entity personnel.

1. Complete the [VPN Requests for External Entities Process](#).
2. Complete the [Ohio Department of Job and Family Services Code of Responsibility form \(7078\)](#).
3. In the **ACCESS REQUESTED** field of the 7078 form select **OTHER access** and write **ODJFS VPN**.

Do not complete the **Social Security No.** field.

Reset Form		OHIO DEPARTMENT OF JOB AND FAMILY SERVICES CODE OF RESPONSIBILITY * PLEASE PRINT *			
NAME: First, MI, Last _____		Agency _____			
Work Phone _____		County _____			
Date of Birth _____		Work Unit _____			
Social Security No. _____		Supervisor _____			
AGENCY TYPE: <input type="radio"/> ODJFS <input type="radio"/> Non-ODJFS State <input type="radio"/> County <input type="radio"/> Local Govt. <input type="radio"/> Private/non-profit <input type="radio"/> Federal					
<input type="checkbox"/> Contract Employee Contract Company Name & Telephone No. _____					
ACCESS REQUESTED: (Local Security Coordinator/Supervisor use only)					
<input type="checkbox"/> ODJFS network / email access		<input type="checkbox"/> CRISE	<input type="checkbox"/> SETS	<input type="checkbox"/> FACSIS	
<input type="checkbox"/> MMIS					
OTHER access: ODJFS VPN ← Enter ODJFS VPN in the OTHER ACCESS field					
Novell Container: _____		Novell ID's: _____			

Important: Failure to enter **ODJFS VPN** in the **OTHER access** field will delay your request.

4. Determine your next step:
 - a. If you are requesting site-to-site access to the network, go to step 5.
 - b. If you do not need site-to-site access, continue with step 6.
5. Contact the [MIS Customer Service Center](#) to open a ticket. Request site-to-site VPN access and request a BNS Pre-Production review of the request.

6. Follow the mailing/faxing instructions at the bottom of the **Code of Responsibility** form.

Once your request is received, it will be processed in the order it was received.

The secure token(s) will be delivered to you.

VPN Requests for External Entities Personnel

The following information must be provided with ALL requests for VPN access:

Project/Initiative Information

1. Identify the name of the ODJFS sponsor / project manager. (This person will be responsible for notifying Information Security Unit (INFOSEC) of personnel changes, contract expiration date, contract extensions, etc.)
2. If secure tokens are needed, who is the ODJFS manager responsible for distributing and collecting the secure token(s) when the job is complete?
3. What is the business purpose or driver of this access?
4. Provide the dates when the service is needed (contract dates) or a project plan that shows the lifecycle of the project (start/end dates, delivery dates for software/hardware or documentation).
5. If this is a county initiated request, was a TSSP request submitted (which includes approval from a county director)?
6. Please confirm that an appropriate agreement is in place with the entity and ODFJS, Office of Contract and Acquisitions. The agreement must contain appropriate Business Associate language provisions. See section 4.0 of the ODJFS Security Policy.
7. Will the information they access be shared with a third party? If so, provide a detailed description of the:
 - a. What information is being provided to the 3rd party?
 - b. What is the purpose of sharing the information?
 - c. Primary contact name, number information?
 - d. Names of all those at the third party site who have access to the information?

Company and External Entity Information

1. Company name and corporate address?

Company Name	
Company Address	
Company Phone	
Company Web Address	

2. Please enter a company name or acronym, up to ten characters:

Note: The company acronym will be combined with the standard external entity ID to make the external entity's external ID. For example, *IBM-smiths*, *NORTEL-jonesb02*. A shorter acronym will spare your users the chore of typing in a long user id every time they log onto the system.

3. Who is the key contact at the company? Provide name, title, email address, and phone number(s).

Name	
Title	
Email	
Phone	

4. Who are the company employees and/or subcontractors who will be accessing information? Provide name, job description, email address, phone number(s), and location where the work will be performed.

Name	Job Description	Email	Phone	Location

5. Will external entity be accessing the Internet via a broadband connection? If not, how fast is the connection? (Not applicable for site-to-site VPNs).
6. A description of each IT service and data owners to be made available to the remote external entities (software, IPs, ports, server names, information to be transferred, etc.)?

Software	Server Name	IP	Ports	Information

7. Times and dates when the service is to be available?

8. What devices the external entity will be using to access the network?

Owner	Responsible Person	Device Make	Model	Serial Number	Date introduce into service on the ODJFS network

9. Please complete this section if this is a site-to-site VPN request. The following table provides configuration information. Enter the **VPN Endpoint IP Address** for your company. Complete the fields for **Destination Hosts/Subnets** and **Ports** for your company.

ODJFS to (Name of Company)			
Method of Connectivity		Location of JFS VPN Endpoint	
Site to Site		AirCenter	
VPN Configuration			
ODJFS VPN Endpoint IP Address		(Company) VPN Endpoint IP Address	
156.63.134.5		xxx.xxx.xxx.xxx	
Configuration Details (minimum requirements—ODJFS will negotiate up, on a case-by-case basis)			
IKE Parameters (minimums filled in)		IPSec Parameters (minimums filled in)	
Authentication	Pre-shared Key	Key Exchange	ISAKMP
Encryption	3-DES	Encryption	3-DES
Hash	SHA-1	Hash	SHA-1
Diffie-Hellman Group	2 – 1024	PFS	Group 2
Lifetime in Seconds	86,400	Lifetime in Seconds	28,800
Destination Hosts/Subnets			
ODJFS Hosts/Subnets	Ports	(Company) Hosts/Subnets	Ports

Special Requests

If this access requires any changes to the existing infrastructure, the manager must take the proposed changes through the first phase of MIS Bureau of Network Support (BNS) Technical Review.

1. The sponsor/project manager submits the documentation from the Project/Initiative Information section and the results of the first phase of MIS Bureau of Network Support (BNS) technical review to the Security Architect. The Security Architect determines whether the request should be reviewed by the Security Committee. Once the request is reviewed by the committee, the Security Architect makes a recommendation to the Chief Security Officer for approval. The security architect is then responsible for obtaining Deputy Director's office approval.
2. If this access requires any changes to existing infrastructure, the manager must take the proposed infrastructure changes through the second phase of the BNS Technical Review and Change Control committees, after obtaining management approval.

3. Once all the approvals and appropriate charges are determined, the sponsor/project manager completes two ODJFS Code of Responsibility forms (7078). One is signed by the external entity; the second is signed by a manager. When completing the form:
 - a. Print clearly
 - b. Do not enter a Social Security number on the form
 - c. Include the external entity's company name
 - d. Write **ODJFS VPN** in the **OTHER access** field in the **ACCESS REQUESTED** section.

Reset Form

**OHIO DEPARTMENT OF JOB AND FAMILY SERVICES
CODE OF RESPONSIBILITY
" PLEASE PRINT "**

NAME: First, MI, Last _____ Agency _____
 Work Phone _____ County _____
 Date of Birth _____ Work Unit _____
 Social Security No. _____ Supervisor _____

AGENCY TYPE: ODJFS Non-ODJFS State County Local Govt. Private/non-profit Federal

Contract Employee Contract Company Name & Telephone No. _____

ACCESS REQUESTED: (Local Security Coordinator/Supervisor use only)

ODJFS network / email access CRISE SETS FACSIS

OTHER access: _____

Novell Container: _____ / Novell ID's: _____

4. The sponsor/project manager submits the information, from the Project/Initiative Information section, the 7078 forms, and documentation of the approvals from a Deputy Director and Security Office to INFOSEC. Requests can be faxed to (614)995-0118 or mailed or to:

Ohio Department of Job and Family Services
 BNS/Information Security Unit
 4200 East Fifth Avenue
 Columbus, Ohio 43219-2551

5. The requests are provisioned in the order in which they are received. ODJFS does not provide external entities with GroupWise or Novell access.
6. External entities are restricted to specific devices according to their role and only have access to the devices they need to perform their duties. This is accomplished when the NOC creates a customized group and profile on the VPN concentrator. The profiles are emailed to the sponsor/project manager. The VPN software and instructions are available at R:\MIS\PRIVATE\OTPO\Projects\Current\Remote VPN Access\External entityCD. The sponsor/project manager should burn the profile, software, and instructions on a CD.

7. For non-site-to-site VPN requests: The tokens are provided to the ODJFS manager responsible for the external entity.

Distributing the Secure Tokens (non-site-to-site VPN requests)

The sponsor/project manager must follow the steps outlined below to distribute the token(s).

- a. If the external entity is out of town, the token is mailed via DHL. The PIN is given to the external entity over the phone if the token is mailed. The token, PIN and ID should never be mailed together.
- b. If the external entity can come to the Air Center, we give them the CD, PIN, and ID at the same time.

VPN Support

The external entity will not receive any support from ODJFS, and ODJFS does not install software for the entity. The external entity must rely on the ODJFS manager responsible for the external entity for assistance. ODJFS does provide informative instructions for the external entity.

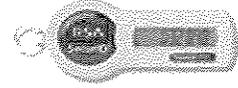
Managing the VPN Access

The sponsor/project manager is responsible for informing INFOSEC when access can be terminated (when the project is done or the person is no longer with the external entity).

ODJFS will conduct periodic reviews to verify access.

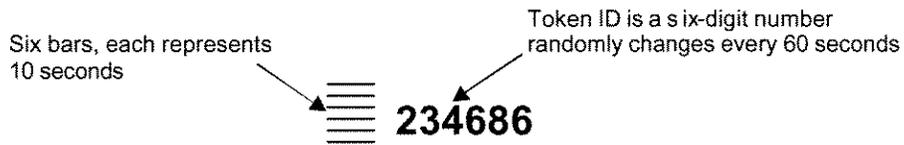
The Secure Token

After submitting the VPN request, the paperwork is processed in the order in which it is received. Once the paperwork is complete, a secure token is assigned to you. This token will have a specific serial number on the back of the token and will be provisioned with a Personal Identification Number (PIN). Each time you log into the network from a remote location, you will use your PIN to gain access to the ODJFS network.



Your PIN is private. Sharing your secure token and PIN with another person is not permitted. Sharing tokens is a violation of ODJFS policy, the Ohio Revised Code, and Federal IRS codes.

The front of the secure token has a window. The window displays a six-digit number known as a Token ID. This number changes every 60 seconds. On the left side of the window are a series of six bars. Each bar represents 10 seconds. Every 10 seconds one bar disappears, until all six are gone. When all of the bars are gone, a new six-digit number randomly appears, with six bars.



Using the VPN to Log Into the ODJFS Network

Before You Begin

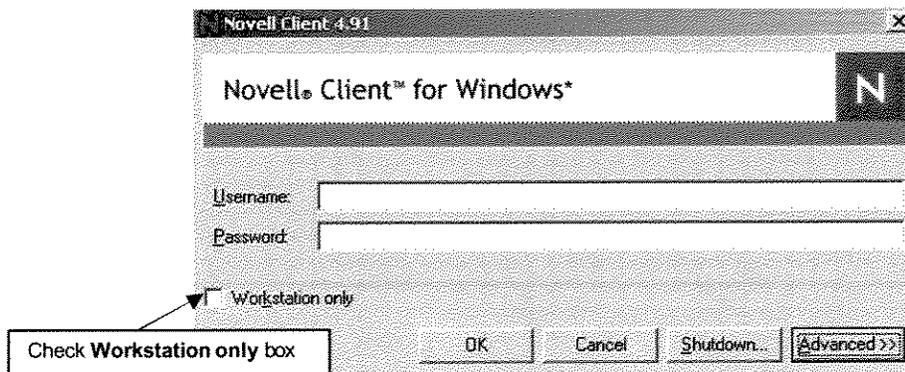
You must connect your laptop to a high-speed network such as Road Runner or using a network connection to a LAN line, a W-Fi connection to an Internet Service Provider (ISP), or via an Air-Card with sufficient bandwidth to support the establishment of the VPN connection. VPN does not work using a land line (regular phone line).

When you access the ODJFS network, you must complete these steps:

- Use the VPN to access the ODJFS network
- Authenticate your user ID on the network
- Regularly scan the State-owned laptop to protect it from viruses.

Using the VPN to Access the ODJFS Network

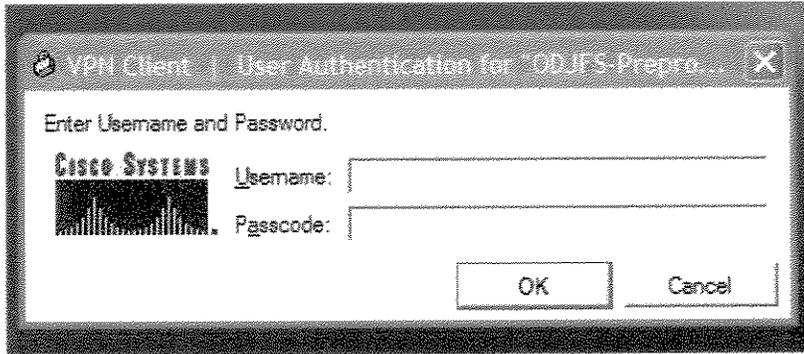
1. Power up your laptop. When the system displays the **Novell Client** login window your Novell ID may appear in the **Username** field. Enter your Novell password in the **Password** field, check the **Workstation Only** box and click .



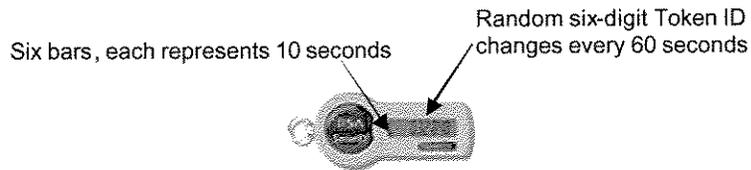
Note: If your **Workstation Only** and **Novell** logon passwords are not synchronized, the **Workstation Only** password may be different than your Novell password.

2. Double click the **Step One-VPN Client** icon  on your desktop.

The system displays the **VPN Client** window.

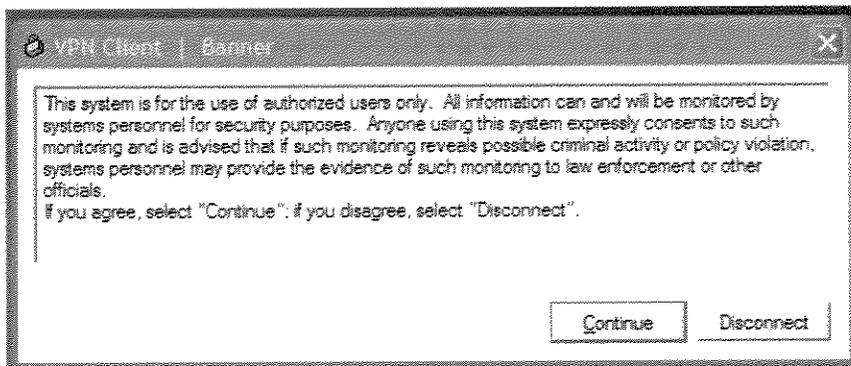


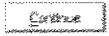
3. Verify your Novell ID in the **Username** field. If the field is blank, enter your Novell ID.
4. Look at your secure token. It will display a six-digit number (Token ID) and a series of bars to the left of the number.



5. In the **Passcode** field enter your assigned four-digit PIN and six-digit Token ID in the secure token window with no spaces between the two, for example 5555123456.
6. Click .

The system displays the **VPN Client Banner** consent form.



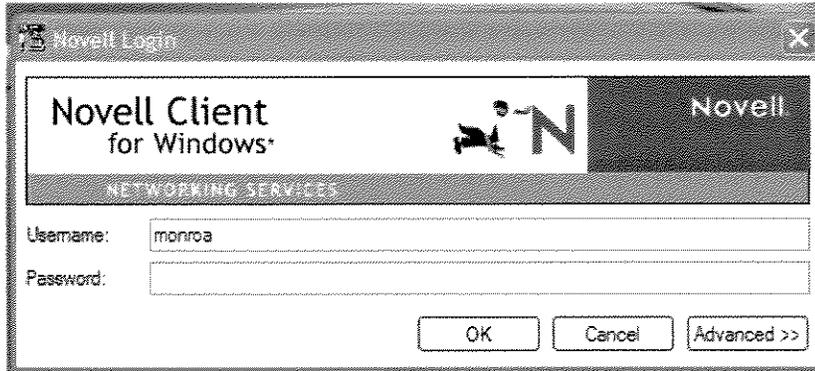
7. Click .

You are now inside the ODJFS network. Next, the system must authenticate your Novell ID.

Authenticating Your Novell ID on the Network

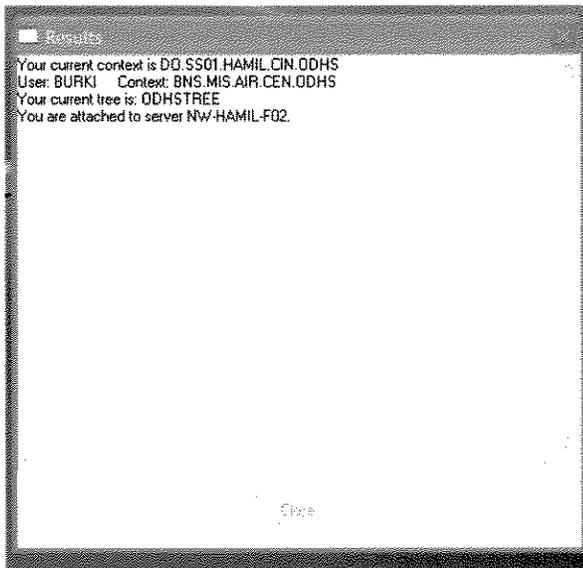


1. Click the **Step Two-Novell Login** icon on the desktop.
The system displays the **Novell Client for Windows** login window. Your Novell ID will appear in the **Username** field.

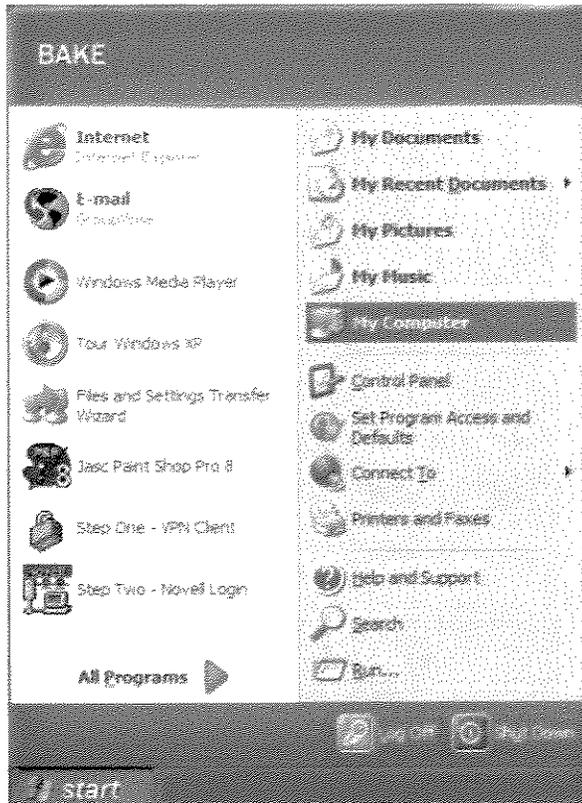


2. Enter your Novell password in the **Password** field.
3. Click .

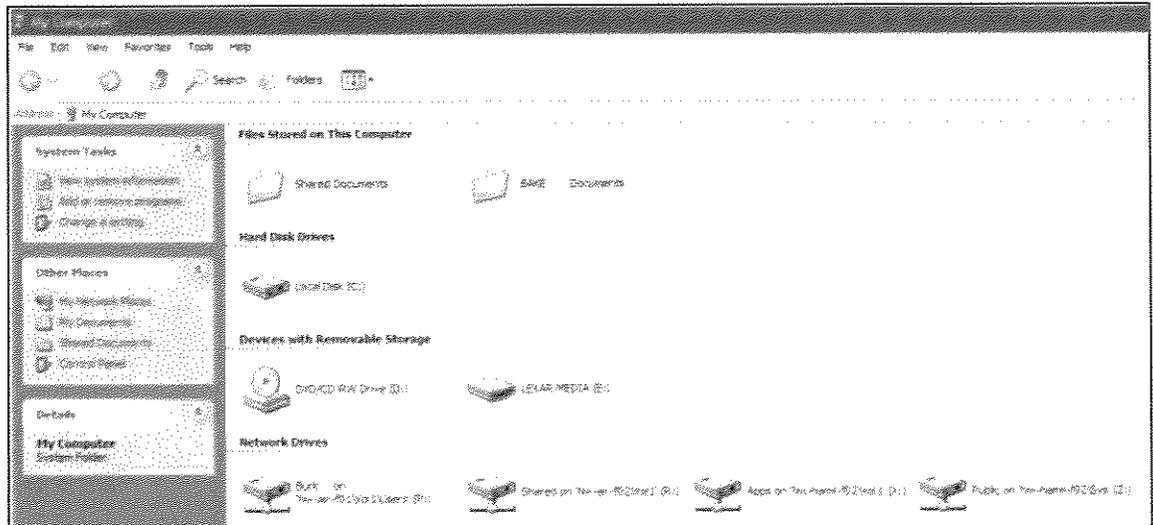
The system displays the **Results** window, authenticates your Novell login ID, and then closes the window.



- To open, click the Start menu  and select **My Computer**.



The system displays your files and folders.



Protecting the Software on the State-Owned Laptop

Ensure that the antivirus software profiles on the State-owned laptop is current. Scan the laptop regularly for viruses. For more information, see the [State of Ohio IT Policy Portable Computing Security](#).

Replacing an Expired Secure Token

The secure tokens have an expiration date. The expiration date is on the back of the token, below the serial number. To prevent an interruption in service, a new token must be obtained prior to the expiration date. The replacement token is issued to the owner of the expiring token.

1. Send an e-mail message to the Information Security Office at INFOSEC@odjfs.state.oh.us and include the following information:
 - a. The name person who owns the token
 - b. The token serial number. This can be found on the back of the token.
 - c. The date the token will expire. The can be found on the back of the token, below the serial number.

When the new token is registered to the owner before the expiration date, the PIN remains the same.

When the new token is registered after the expiration date, a new PIN must be issued.