User Guide
Go-Remote Access Service

Complete Guide for Registering and Accessing the OPS Network

Version 1.4
June 12, 2017
Table of Contents

1) Introduction ........................................................................................................................................ 4

2) Registration Process for OPS Employees .......................................................................................... 4
   2.1 S.ODO Request for GO-Remote Access Service ........................................................................... 5
   2.2 Invitation to Register for GO-Remote Access Service – Registration Link and Code ............. 5
   2.3 Online Authentication and Registration ....................................................................................... 6
       2.3.1 Subscriber Agreement Acceptance and Digital Signature ................................................... 7
       2.3.2 User Information Confirmation ............................................................................................. 7
       2.3.3 Completion ........................................................................................................................... 8
   2.4 Receive User ID and SafeNet Token ............................................................................................... 8
   2.5 Register SafeNet Token ................................................................................................................ 9
   2.6 Access the OPS Network ..............................................................................................................10
   2.6 Network Shared Drives ...............................................................................................................11

3) Registration Process for Non-OPS Employees ..................................................................................12
   3.1 S.ODO Request for GO-Remote Access Service ........................................................................13
   3.2 GO-Security Token Request Form ...............................................................................................14
   3.3 Uploading the Forms .....................................................................................................................14
       3.3.1 Logging into the GO-Remote website ......................................................................................14
       3.3.2 Upload Approved Forms .......................................................................................................15
       3.3.3 Mailing the Forms ................................................................................................................16
   3.4 Complete Authentication and Security Profile – Registration Link and Code ..............................17
       3.4.1 Secret Questions and Answers Creation ..................................................................................17
       3.4.2 User Information Confirmation .............................................................................................18
       3.4.3 Completion ...........................................................................................................................19
   3.5 Receive User ID and SafeNet Token ...............................................................................................20
   3.6 Register SafeNet Token ................................................................................................................20
   3.7 Download Cisco AnyConnect and Access the OPS Network .........................................................23
       3.7.1 Navigate to the GO-Remote Website ......................................................................................23
       3.7.2 Read the Login Disclaimer and click "Continue" ....................................................................24
       3.7.3 Install AnyConnect ...............................................................................................................24
       3.7.4 Begin Install Process ..............................................................................................................24
3.7.5A Java Method ........................................................................................................25
3.7.5B Manual Method ........................................................................................................25
3.7.5B-1 Save the AnyConnect EXE File ........................................................................26
3.7.5B-2 Install the AnyConnect EXE File .........................................................................26
3.7.5B-3 Launch Cisco AnyConnect ..................................................................................27
3.7.5B-4 Connect to OPS Network .....................................................................................27

4) Logging into the OPS Network .....................................................................................28
   4.1 Network Shared Drives .............................................................................................28
   4.2 Disconnecting from the OPS Network .......................................................................29

5) Online Self-Administration ..........................................................................................29

6) Returning Old or Defective Tokens ..............................................................................30

7) Contacts for Support ...................................................................................................30

8) Document Revision History ........................................................................................31
1) Introduction

GO-Remote Access Service is a secure connection to the Ontario Public Service (OPS) network when working remotely from the office. Once connected, you will be able to access the same network resources (e.g., Ministry systems and shared drives) the same way you normally would in an OPS office.

This guide is for OPS employee and Ministry sponsors/ managers who are applying on behalf of a non-OPS employee, for GO-Remote Access Service. This guide explains the process of registering for the service and its use.

If you were contacted to register for the new GO-Remote Access Service because your current service was granted prior to May 2017, please consult these Frequently Asked Questions or visit InsideIT.

2) Registration Process for OPS Employees

The following process is for all OPS employees (and a small number of others) who have GO-PKI security credentials for logging into WIN.

Important: For re-registration from the old VPN service to the new GO-Remote Access Service please skip to Section 2.5 –Receive User ID and SafeNet Token
2.1 S.O.DO Request for GO-Remote Access Service

The process starts with the submission and approval of the request for GO-Remote Access Service for an OPS employee through the Service Order Desk Online (S.O.DO):

1. Visit [S.O.DO](#) and select “All Products and Services”
2. Confirm your organization (i.e. Ministry)
3. Select “Networking Services”
4. Select “GO-Remote Access Services”
5. Under “GO-Remote VPN (Individual User Accounts)” Services” select “Add to Cart”
6. Under “Request Type” select:
   a. “Add New VPN Service” access
7. Complete the user information based on the request that appears, then hit save

Once your Ministry program area’s approver (manager) approves your request, GO-Remote Administration, Infrastructure Technology Services will email you directly to register for GO-Remote Access service.

2.2 Invitation to Register for GO-Remote Access Service – Registration Link and Code

A) An email with a registration link is sent to the address provided by you in your S.O.DO request.

B) A registration code will be sent in a separate email. You must use Internet Explorer to open the registration link and use your registration code to complete your authentication.
Three registration reminders will be emailed to you. Your request will be cancelled if you do not complete your registration within 30 days.

2.3 Online Authentication and Registration

Follow the link in the registration notification email using Internet Explorer to begin self-registration.

You will be directed to a GO-PKI login page where you must log in using your credentials, the same way you log into WIN:

- Locate your GO-PKI profile
- Enter your GO-PKI password
- Click “Sign In”
2.3.1 Subscriber Agreement Acceptance and Digital Signature

Read the terms and conditions of use, and then verify your agreement using the tick-box at the bottom of the page.

By checking this 'Agreement' check box I agree with the terms of the Subscriber Agreement for the RAS/VPN "GO Remote" service and I digitally sign my acceptance.

2.3.2 User Information Confirmation

Then confirm your user details and your mailing address — this information will be used for your User ID and to send your SafeNet token.
The Client information section will have all your client information as submitted by S.ODO. The
Token mailing address will be used to mail you your new SafeNet Token. You can choose your office address if you would like your new token to go to your office location.

2.3.3 Completion

You have now completed your registration and will receive an email from
GORemote.Administration@ontario.ca with your credentials and next steps.

2.4 Receive User ID and SafeNet Token

You will receive an email with your User ID (the email address you supplied) and a hyperlink that you will need to access to complete your registration.

Meanwhile a SafeNet token, which is used for generating temporary codes for logging into the OPS network, will be mailed to your address in 5-10 business days. The token can only be used by you.
2.5 Register SafeNet Token

Once you receive your new SafeNet token in the mail using Internet Explorer (other browsers will not work):

1. Visit [INSERT URL].
2. Enter your User ID: [INSERT EMAIL ADDRESS]
3. Enter the new SafeNet token serial number (located on the back of your new token).
4. Create and enter a four-digit Personal Identification Number (PIN).
5. Press the “Activate” button. You should receive a confirmation that your token is successfully activated.

You must activate your token within 30 days from when you received your “VPN Token User ID” email or your request will be cancelled (see 2.4 - Receive User ID and SafeNet Token).
Existing Users Who are Activating a New SafeNet Token Remotely

1. Login to the OPS network using the current VPN process.
2. Follow steps in 2.5 Register SafeNet Token.
3. Once your new token is activated, you need to logout of your current VPN connection and log back into VPN using your new SafeNet token and the AnyConnect application (see 2.6 Access the OPS Network)

2.6 Access the OPS Network

You can now use your token to log into GO-Remote VPN Access Service.

Cisco AnyConnect is a program installed on all OPS computers for creating a secure connection to the OPS network.

How to use your new SafeNet token (Windows 7 users):

1. Click the Start menu in the bottom left corner of your taskbar.
2. Locate “OPS Remote Access Service.”
3. Click “Cisco AnyConnect Secure Mobile.”
4. Enter the email address you used to register for the GO-Remote Access Service.
5. Enter your passcode, which is your four-digit PIN and the current six digits displayed on your SafeNet token (the six digits will change when the button is pressed on the token).
How to use your new SafeNet token (Windows 10 users):

1. Click the Windows icon in the bottom left corner of your taskbar.
2. Locate and click “All apps.”
3. Locate and click “OPS Remote Access Service,” and then click “Cisco AnyConnect Secure Mobile.”
4. Enter the email address you used to register for the GO-Remote Access Service.
5. Enter your passcode, which is your four-digit PIN and the current six digits displayed on your SafeNet token (the six digits will change when the button is pressed on the token).

If you cannot locate Cisco AnyConnect, please contact the OPS IT Service Desk.

2.6 Network Shared Drives

Once you connect to the OPS network through Cisco AnyConnect, your network shared drives should be available automatically.

However, in some instances, network shared drives may not be immediately available after remote login. If your network shared drives are not available after you login through Cisco AnyConnect, either

1. Follow the self-service option to reconnect your drives.

   Or

2. Contact the OPS IT Service Desk at 416-246-7171 or 1-888-677-4873

Once you log off your remote connection to the OPS network, you may lose access to your network shared drives again. To avoid this issue, do not shut down your mobile PC between uses. Instead, use hibernate/sleep mode.
3) Registration Process for Non-OPS Employees

The following process is for non-OPS employees who do not have GO-PKI security credentials and must follow a different process to establish their credentials.

START

S.ODO request for non-OPS employee access is submitted and approved

Approving manager emailed GO-Security Token Request Form and instructions for non-OPS employee

Non-OPS employee submits complete form and supporting documents to approving manager

Approving manager submits non-OPS employee’s form and documents to ITS

ITS receives non-OPS employee’s documents for validation & verification

Vendor emailed registration invitation

Non-OPS employee registers on GO-Remote website and sets up security profile

User ID and registration hyperlink emailed to non-OPS employee

GO-Remote token mailed to non-OPS employee

Non-OPS employee registers token using user ID and link

Non-OPS employee uses token to access and install Cisco AnyConnect to access the OPS network

COMPLETE
3.1 S.ODO Request for GO-Remote Access Service

The process starts with the submission and approval of the service request for GO-Remote VPN (Individual User Account) Service for a non-OPS employee through the Service Order Desk Online (S.ODO): Non-PKI users (non-OPS employees) cannot fill in the S.ODO order for this service by themselves. The Ministry sponsor/manager will have to submit the S.ODO order on their behalf.

1. Visit S.ODO and select “All Products and Services”
2. Confirm your organization (i.e. Ministry)
3. Select “Networking Services”
4. Select “GO-Remote Access Services”
5. Under “GO-Remote VPN (Individual User Accounts)” select “Add to Cart”
6. Under “Request Type” select “Re-Register Existing VPN Account”
7. Enter the non-OPS employee’s User ID (i.e. email address)
8. Under “Is this request for an OPS employee?” select “No”
9. If the non-OPS employee does not have GO-PKI certificate select “No” and follow the directions

Once the S.ODO request is approved, GO-Remote Administration will email the Ministry sponsor/manager with directions to provide to the non-OPS employee.

---

Dear,

This is to advise you that your S.ODO request to grant GO-Remote Access Service to a non-OPS employee was successfully processed.

What Happens Next

1. Your ministry and the non-OPS employee must now complete the GO-Security Token Request Form:
   https://stage.gopssregistration.gov.on.ca/VPNManagerUpload?email=

   After the form and supporting documents are validated, we will contact the non-OPS employee via email to complete the registration process and provide them with a SafeNet hard token.
3.2 GO-Security Token Request Form

GO-Remote Administration then emails the Ministry program area. The email includes a GO-Security Token Request Form to be completed by the non-OPS employee. The non-OPS employee is required to provide three supporting documents to establish the non-OPS employee's identity.

The non-OPS employee submits these documents to the Ministry approving manager to submit to ITS.

3.3 Uploading the Forms

The Ministry approving manager must upload the completed GO-Security Token Request Form and the non-OPS employee’s supporting documentation to the GO-Remote website.

The documents and form should be saved as PDFs.

3.3.1 Logging into the GO-Remote website

The Ministry approving manager will be directed to a GO-PKI login page where they must use Internet Explorer and log in using their credentials, the same way you log into WIN:

- Locate your GO-PKI profile
- Enter your GO-PKI password
- Click “Sign In”
3.3.2 Upload Approved Forms

Once the GO-PKI login is successful you will see the GO-Remote website below where you will see a list of all Service Requests that have pending form and supporting documentation uploads.

1. Select your Request ID from the list. You may sort this list by “Request ID”, “Request Status”, “RAS Account Expiry Date” and “Modified On”

2. User information will be pre-populated with the NON-OPS User information provided in the S.ODO request.

3. Use the “Browse” button to navigate to the PDF file(s) that is composed of the completed GO-Security Token Request Form and the supporting documents in a single file.
4. If the upload is successful a confirmation message will be presented, and the non-OPS employee will be contacted directly by GO-Remote Administration to complete their registration.

3.3.3 Mailing the Forms

In the event that the forms upload cannot be completed, the Ministry approving manager, can mail the forms as a backup.

The form and supporting documents can be sent via the OPS internal mail to:

GO-Remote Access Service Support
Infrastructure Technology Services
Telecommunication Services Branch
222 Jarvis Street 6th Fl.
Toronto, ON M7A 0B6
3.4 Complete Authentication and Security Profile – Registration Link and Code

1. An email with a registration link is sent to the non-OPS employee.

2. A registration code is sent to the non-OPS employee in a separate email. The registration link and the registration code must be used to complete the authentication process.

The new client will be directed to an authentication page where they must correctly answer the user identification questions that were captured in the GO-Security Token Request Form.

3.4.1 Secret Questions and Answers Creation

The non-OPS employee then creates a security profile using a list of personal questions. They have to provide answers to five (5) of these questions. They will need these answers every time they interact with the Self Administration system (i.e. when changing the PIN or requesting a token replacement.)
3.4.2 User Information Confirmation

The non-OPS employee confirms their user details and mailing address. This information is used to establish their User ID and to mail out their SafeNet token.
Three registration reminders will be emailed directly to the new user. The request will be cancelled if they do not complete their registration within 30 days.

3.4.3 Completion

Registration is now complete and the non-OPS employee will receive an email from GORemote.Administration@ontario.ca with their credentials and next steps.
3.5 Receive User ID and SafeNet Token

You will receive an email with your User ID (the email address you supplied) and a hyperlink that you will need to complete your registration.

Meanwhile a SafeNet token, which is used for generating temporary codes for logging into the OPS network, will be mailed to your address within 5-10 business days. The token can only be used by you.

3.6 Register SafeNet Token

The non-OPS employee receives their SafeNet token in the mail and activates it using the hyperlink received in the VPN Token User ID email:

What happens next:
1. You will receive your SafeNet token in the mail
2. You will activate your token here: [https://gomeznombre.com](https://gomeznombre.com)
3. Enter your User ID
4. Enter the token serial number (engraved on the back of your new token)
5. Enter your 16 digit Personal Identification Number (PIN) that you will be using for logging into the OPS network

If you already have Cisco AnyConnect installed and need help configuring it please contact your own IT support office.
1. Enter User ID

2. Answer 3 of the Secret Questions that were selected during the Registration Process (step 3.4.1). Note, you may only skip 1 question.

3. Enter the token serial number (on the back of the new token)

4. Enter the 4 digit Personal Identification Number (PIN) that will be used for logging into the OPS network
The user must activate their token within 30 days from when the user received their “VPN Token User ID” email or their request will be cancelled (see 3.5 Receive User ID and SafeNet Token).

Existing Non-OPS Employees Who are Activating a New SafeNet Token Remotely

1. Login to the OPS network using the current VPN process.
2. Follow steps in 3.6 Register SafeNet Token.
3. Once your new token is activated, you need to logout of your current VPN connection and log back into VPN using your new SafeNet token and the AnyConnect application (see 3.7 Download Cisco AnyConnect and Access the OPS Network)
3.7 Download Cisco AnyConnect and Access the OPS Network

Cisco AnyConnect is a program used for creating a secure connection to the OPS network. Non-OPS employees must download and install Cisco AnyConnect.

**Note:** Windows 7 (32&64bit), 8.1 (32&64 bit) and Windows 10 are the supported and tested platforms. Installing the package on any other platform is the responsibility of the non-OPS employee and may produce unfavorable results.

If you already have Cisco AnyConnect installed and need help configuring it please contact your own IT support office.

3.7.1 Navigate to the GO-Remote Website

Non-OPS employees must go to:

- [https://goremotegdc.gov.on.ca](https://goremotegdc.gov.on.ca) or
- [https://goremotekdc.gov.on.ca](https://goremotekdc.gov.on.ca)

and enter the user credentials that were set up during the GO-Remote Access Service registration:

- Email: Enter your username (i.e. email address)
- Passcode: Enter your 4 digit PIN + the six digits currently displayed on your SafeNet token
3.7.2 Read the Login Disclaimer and click “Continue”

3.7.3 Install AnyConnect

In the left navigation Pane select “Install AnyConnect”

3.7.4 Begin Install Process
Click Start AnyConnect in order to begin the installation process.

The installer will first check if your computer has the appropriate JAVA software installed.

3.7.5A Java Method

If the Web installer detects an out-of-date version of JAVA, you are not required to update JAVA. Click “LATER” to continue installing AnyConnect via JAVA.

When complete, you will launch AnyConnect and establish a connection to the OPS network (see 4 - Logging into the OPS Network).

3.7.5B Manual Method

If your computer is not running JAVA you will be prompted to follow the manual install process — click the “AnyConnect VPN” link to download the AnyConnect EXE file.
3.7.5B-1 Save the AnyConnect EXE File

Save the AnyConnect EXE file to your computer and then run it to install Cisco AnyConnect.

The EXE file may be in your “Downloads” folder or perhaps your browser will prompt you when the download is complete and ready to be installed. i.e. in Firefox:

3.7.5B-2 Install the AnyConnect EXE File

The downloaded file is called “anyconnect-win-4.3.00748-web-deploy-k9.exe”

Double click the file to run the installation and follow the instructions.
Once installed, click “Finish”

3.7.5B-3 Launch Cisco AnyConnect

Launch the fresh install of Cisco AnyConnect Secure Mobility Client, from the Start menu

3.7.5B-4 Connect to OPS Network

Under “VPN” enter either:

- goremotegdc.gov.on.ca or
- goremotekdc.gov.on.ca

NOTE: You will only need to do this when you install Cisco AnyConnect. In the future “OPS Enterprise RAS” will automatically appear here.
4) Logging into the OPS Network

Once your SafeNet token is activated and you have started Cisco AnyConnect, you can log into the OPS network:

- Enter your email address
- In the Passcode field enter:
  - Your four digit PIN and the six digits currently displayed on your SafeNet token

You will create a secure, remote connection to the OPS network. Once connected, you will be able to access the same network resources (e.g., Ministry systems and shared drives) the same way you normally would in an OPS office.

4.1 Network Shared Drives

Once you connect to the OPS network through Cisco AnyConnect, your network shared drives should be available automatically.

However, in some instances, network shared drives may not be immediately available after remote login. If your network shared drives are not available after you login through Cisco AnyConnect, either

1. Follow the self-service option to reconnect your drives.

Or

2. Contact the OPS IT Service Desk at 416-246-7171 or 1-888-677-4873

Once you log off your remote connection to the OPS network, you may lose access to your network shared drives again. To avoid this issue, do not shut down your mobile PC between uses. Instead, use hibernate/sleep mode.
4.2 Disconnecting from the OPS Network

You can disconnect from the OPS Network by selecting the “Cisco AnyConnect” icon that can be found in the “show hidden icons” area in the bottom right corner of the Windows task bar.

Once the Cisco AnyConnect Secure Mobility Client window is open, hit the “Disconnect” button found on the right hand side.

5) Online Self-Administration

The GO-Remote website can also be used to change your PIN or to request a new Safenet token.

Simply click on “Self-Administration”, use your credentials and follow the directions.

You can also access the Self-Administration page from S.ODO page by using the following steps:

1. Visit S.ODO and select “All Products and Services”
2. Confirm your organization (i.e., Ministry)
3. Select “Networking Services”
4. Select “GO-Remote Access Services”
5. “To replace lost or damaged token or change PIN click here.”
6) Returning Old or Defective Tokens

If you have an old RSA SecurID token, it will not work with the new VPN access system. Please return RSA SecurID or defective tokens to:

GO-Remote Access Service Support
Infrastructure Technology Services
Telecommunication Services Branch
222 Jarvis Street 6th Fl.
Toronto, ON M7A 0B6

7) Contacts for Support

You can contact the OPS IT Service Desk at 416-246-7171 or 1-888-677-4873 for any issues related to this email.
8) Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description of Changes</th>
<th>Contributors</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 10</td>
<td>.10</td>
<td>Initial draft</td>
<td>Katie Topic</td>
</tr>
<tr>
<td>December 29, 2016</td>
<td>.20</td>
<td>Combined OPS and Non-OPS</td>
<td>Dennis Sithoo</td>
</tr>
<tr>
<td>January 4, 2017</td>
<td>.30</td>
<td>Process updates</td>
<td>Dennis Sithoo</td>
</tr>
<tr>
<td>January 6, 2017</td>
<td>.40</td>
<td>Process updates</td>
<td>Dennis Sithoo, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>January 9, 2017</td>
<td>.50</td>
<td>Process updates</td>
<td>Dennis Sithoo</td>
</tr>
<tr>
<td>January 10, 2017</td>
<td>.60</td>
<td>Updated screenshots</td>
<td>Dennis Sithoo, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>January 12, 2017</td>
<td>.70</td>
<td>Process updates</td>
<td>Dennis Sithoo, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>January 18, 2017</td>
<td>.80</td>
<td>Updated screenshots</td>
<td>Dennis Sithoo, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>March 23, 2017</td>
<td>.90</td>
<td>Process updates</td>
<td>Dennis Sithoo, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>April 3, 2017</td>
<td>.10</td>
<td>Updates to links</td>
<td>Dennis Sithoo</td>
</tr>
<tr>
<td>April 24, 2017</td>
<td>1.0</td>
<td>Update to soft token, screenshots</td>
<td>Scott McCormick, Sameh Akladios, Katie Topic</td>
</tr>
<tr>
<td>May 5, 2017</td>
<td>1.1</td>
<td>Update on process change for</td>
<td>Katie Topic</td>
</tr>
<tr>
<td>May 8, 2017</td>
<td>1.2</td>
<td>Update for AODA compliance</td>
<td>Daniel Petrangelo</td>
</tr>
<tr>
<td>June 12, 2017</td>
<td>1.4</td>
<td>Update for AODA compliance</td>
<td>Daniel Petrangelo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added network shared drive reconnection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>instructions</td>
<td></td>
</tr>
</tbody>
</table>