



Entrust IdentityGuard Soft Token Version 1.0 Patch 175434 Installation Guide for Windows

PROPRIETARY AND CONFIDENTIAL

The information contained in this document is legally privileged and confidential to CGI and to the receiving party. This document cannot be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, without the written approval of CGI. The receiving party is exempt from this restriction for evaluation purposes only.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at (+1) 613-740-5900 extension 5411, ask to speak to a CGI Incident Handler and to return this document by certified mail.

Table of contents

1	Introduction	3
1.1	PREREQUISITES	3
1.2	ASSISTANCE	3
2	Installation on workstation	4
3	Registration	10
4	Activation	16
5	FAQ	23
Appendix A - Hardware Token		25
Appendix B - Mobile Installation		26
Appendix C - Cisco VPN		32
Appendix D - ex-Logica Web Portal		34
Appendix E - Avaya VPN Client Connection		37

1 Introduction

Entrust IdentityGuard Soft Token is a mobile identity application to authenticate users without requiring specialized security hardware.

It is meant to be a replacement for the presently used RSA SecurID tokens and the Nordic Edge/McAfee Pledge software tokens.

This document is a user guide for the installation and configuration of Entrust IdentityGuard Soft Token Version 1.0 Patch 175434 for Windows.

It is a 3 step procedure:

- Installation
- Registration
- Activation

These must be followed in sequence as listed.

The approximate time of completion is 20 minutes.

Please confirm that all prerequisites are met before proceeding.

1.1 Prerequisites

In order to complete this installation, ensure that you first meet all of the following:

- An up to date and security compliant Corporate CGI workstation
- Administrator rights on the workstation
- Appropriate VPN profile(s) for CGI « classic » members.
- Connection to CGINet, SERA Connect or Groupinfra, including via your existing remote access solution.

1.2 Assistance

If you have questions or require further assistance with this installation procedure please call the Enterprise User Service Desk (E-USD) at 1-888-571-7211.

For ex-Logica members that connect thru the Web Gateway (Juniper network Connect, Junos Pulse), If you cannot authenticate successfully, please contact your local IS-IT Helpdesk, details of which can be found here: <http://info.global.logica.com/ab/func/is/helpdesk/Pages/default.aspx>

2 Installation on workstation

N.B.: If you received an **Entrust hardware token**, go to **Appendix A (Hardware Token)** to continue the process.

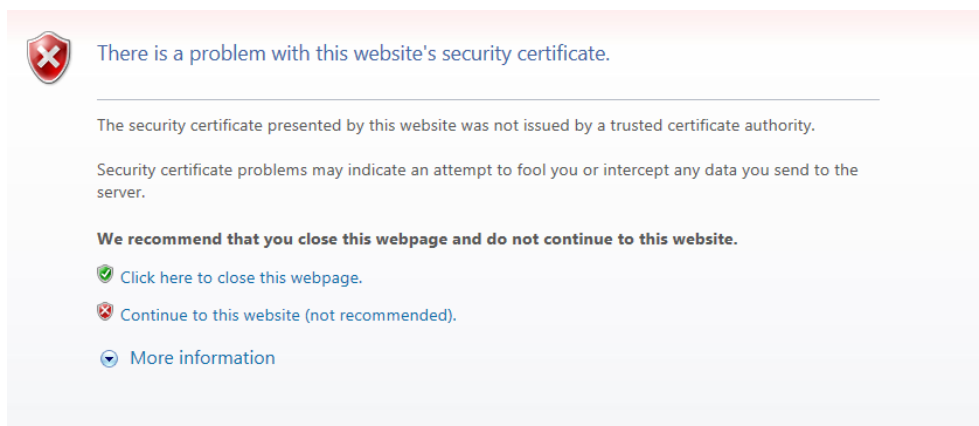
The Entrust soft token can only be installed on one device. Therefore, in order to obtain your token security code, you must have access to the device on which the soft token is being installed.

For example, if you have the ability to connect to a VPN on a secondary workstation (e.g. workstation at home) and, you do not have your primary device (e.g. laptop) with you, you will not be able to connect as your soft token information is on your primary device. For those of you that have a **CGI-provided smart phone**, it is recommended that you install the Entrust soft token on this device.

For installation on the CGI-provided smart phone, consult **Appendix B - Mobile Installation**.

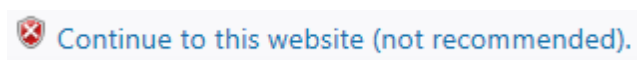
If you are working outside of a CGI office please make sure that you connect through SERA-Connect or your existing Remote Access solution before proceeding.

1. Before proceeding with the installation, ensure that you have access to:



<https://cgientself02.ent.cginet:8445/igdl>

If after clicking on the link you are prompted with the above screen, click on:



2. Select the link corresponding to the device for which you are installing the Entrust IdentityGuard Soft Token.

Note that this installation document describes the procedure to follow for a CGI Corporate workstation configured with Microsoft Windows 7.

Entrust IdentityGuard Mobile Download

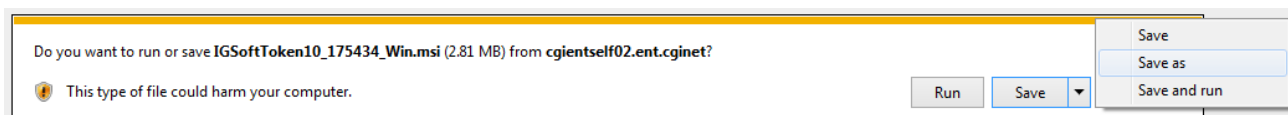
Select the link corresponding to your device. Click [here](#) for help.

- **Android**
- **Apple iPhone/iPod touch/iPad (iOS 3.0 or later)**
- **BlackBerry 10**
- **BlackBerry (O/S 4.7 or later)**
- **BlackBerry (O/S prior to 4.7)**
- **Java Phone**
- **Windows Mobile**
- **Windows XP or Vista or Windows 7**

Additionally, for Windows Phone 8.x, the Entrust App can be downloaded from the Windows Phone Store. For Windows PC 8.x (please follow the same installation instructions as Windows 7)

For installation on the CGI-provided smart phone, consult **Appendix B - Mobile Installation**.

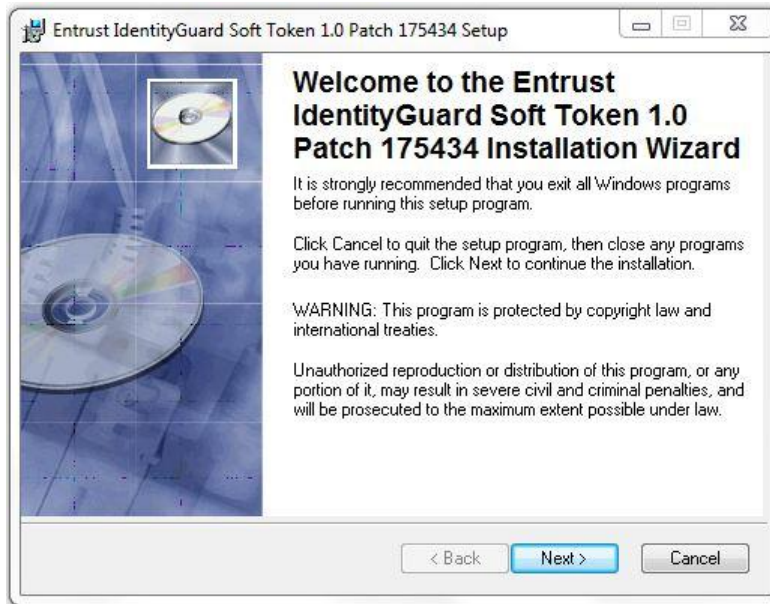
3. After selecting the appropriate device, click on the scroll down arrow of the Save button and choose Save As.



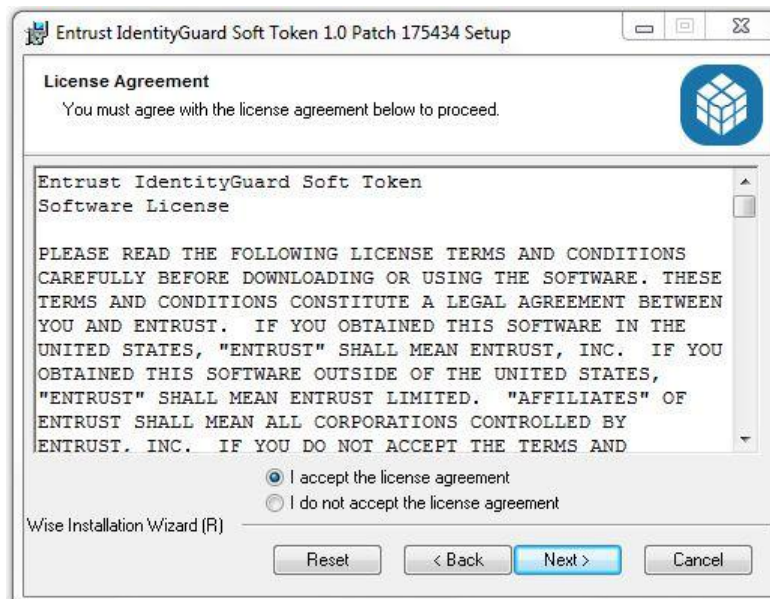
Choose to save the IGSofToken10_175434_Win.msi file on your desktop for easy access.

For members using Internet Explorer 11, you may need to replace the extension with '.msi' to download the file on your desktop only.

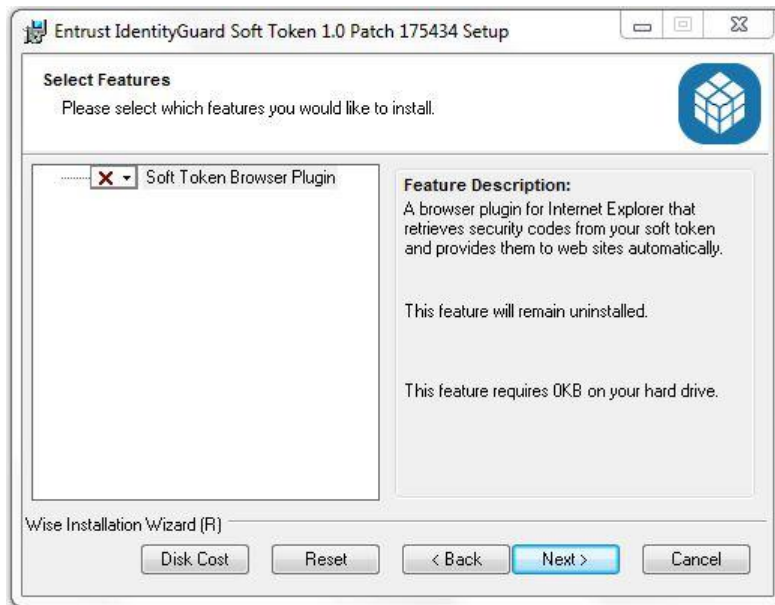
5. After downloading the IGSoftToken10_175434_Win.msi on your desktop, double click it to execute the installation.
6. At the Welcome screen, click the **“Next”** button.



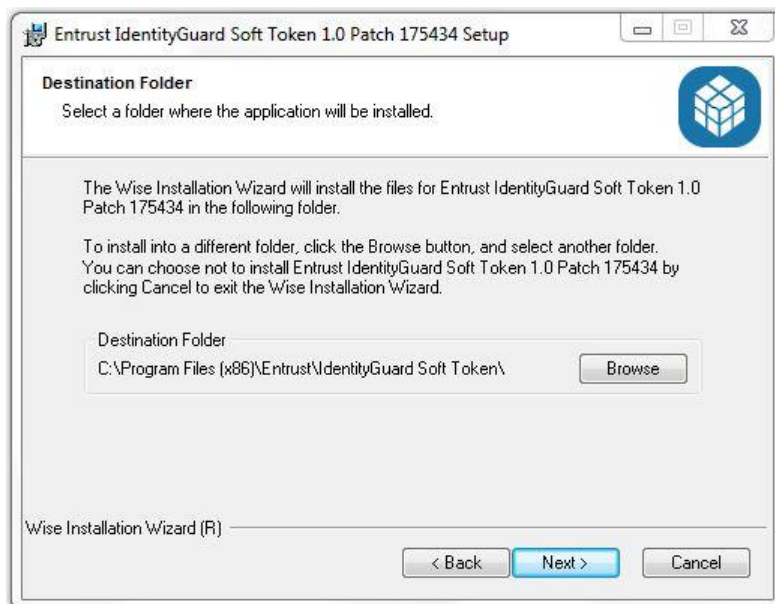
7. Select the radio button **“I accept the license agreement”** then, click the **“Next”** button.



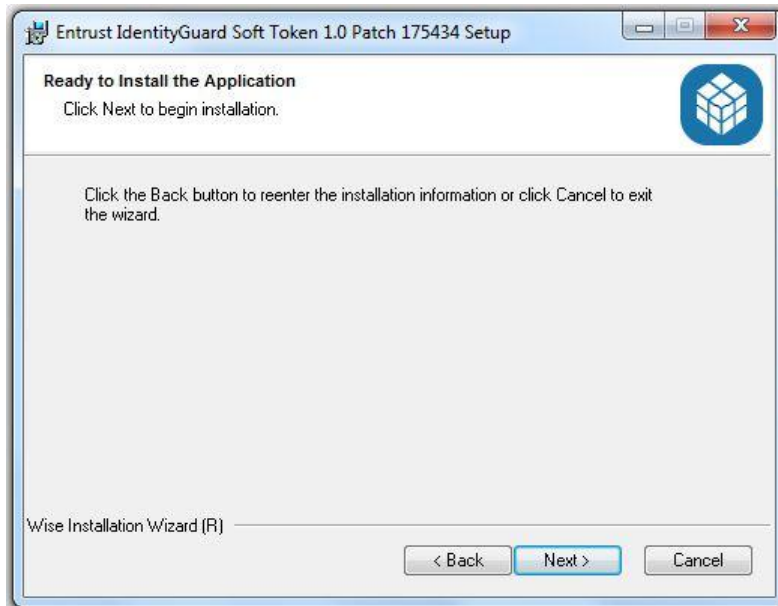
8. Keep default features and click on the **“Next”** button to start the installation.



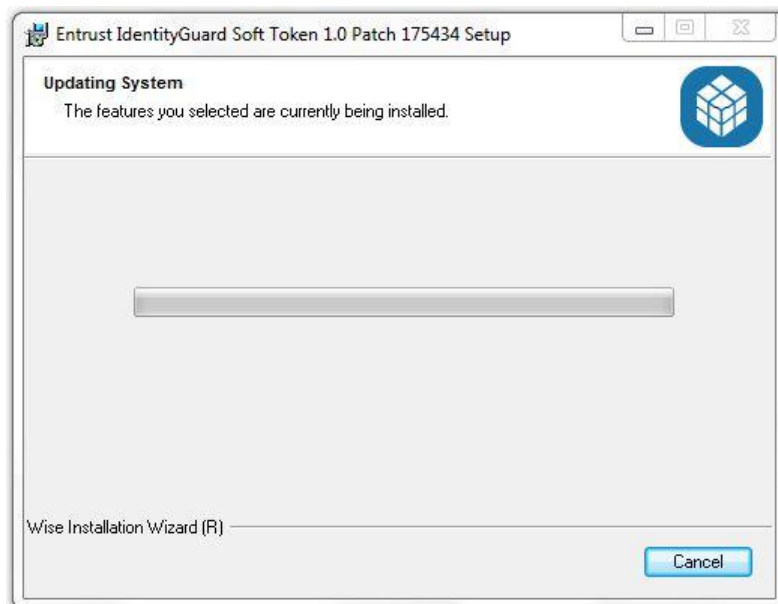
9. Keep the default destination folder and click on the **“Next”** button.



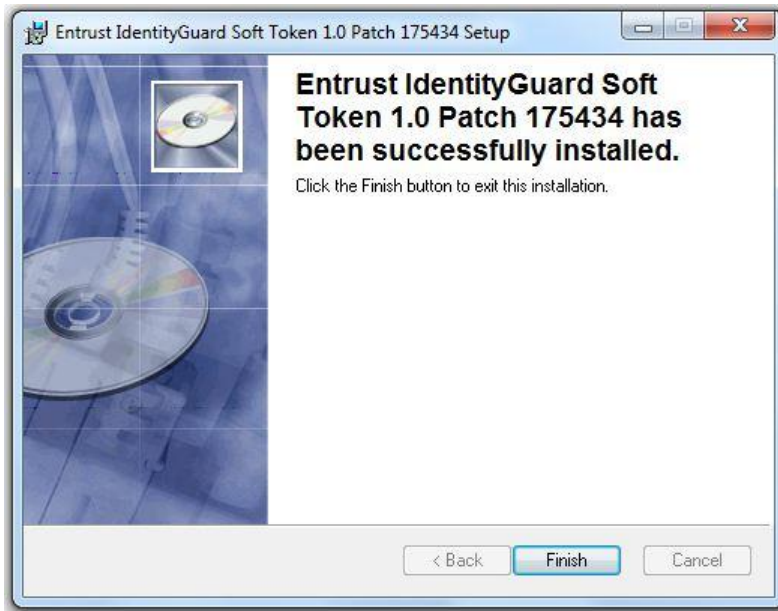
10. Click the **“Next”** button to start the installation.



11. The installation will now proceed. The approximate completion time is 2 minutes.



12. Once the installation is completed, click on the “**Finish**” button.



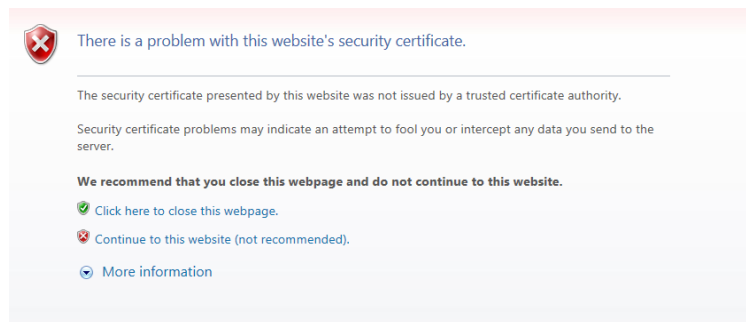
3 Registration

The Entrust IdentityGuard Self-Service registration validates that you are accessing the correct server as well as enabling you to record answers to personal questions to confirm your identity by the Self-Service module. If you are working outside of a CGI office please make sure that you connect through SERA Connect or your usual Remote Access solution before proceeding.

1. Before proceeding with the registration, ensure that you have access to:

<https://cgientself02.ent.cginet:8445/IdentityGuardSelfService/>

(You can **bookmark this URL**, since you can use it in the future to manage your token, thru this self-service site (i.e.: Update personal information, change PVN, etc.))



2. If after clicking on the link you are prompted with the above screen, click on:



3. Enter your credentials

User Name: *firstname.lastname* (The first part of your email address without the @cgi.com).

Password: Your CGI Email/Enterprise Portal password or Groupinfra password.

Then click the Log In button.

Entrust IdentityGuard Self-Service

Log In

* User Name:

* Password:

Please log in to either sign up for multifactor authentication, or to administer your existing account.

Copyright © 2013 Entrust

- From this section, enter your personal information as described in the following pages.

Entrust IdentityGuard Self-Service

Personal Information


Welcome to Entrust IdentityGuard self registration. To begin, please provide the personal information requested below.

* Full Name:

* Contact Information:

Both an email address and a phone number are required.

Delete	Label	Value	Default
<input type="checkbox"/>	Choose label... <input type="text"/>	<input type="text"/>	<input type="radio"/>
<input type="checkbox"/>	Choose label... <input type="text"/>	<input type="text"/>	<input type="radio"/>
<input type="checkbox"/>	Choose label... <input type="text"/>	<input type="text"/>	<input type="radio"/>
<input type="checkbox"/>	Choose label... <input type="text"/>	<input type="text"/>	<input type="radio"/>

Telephone Number Format 

* Mutual Authentication Image:



* Mutual Authentication Phrase:

Next

Copyright © 2013 Entrust

5. Enter your Full Name.

* **Full Name:**

John Smith

6. Enter your Contact Information. Do not select any information as a default. Leave all radio buttons as displayed.

* **Contact Information:**

Both an email address and a phone number are required.

Delete	Label	Value	Default
<input type="checkbox"/>	Email	john.smith@cgi.com	<input type="radio"/>
<input type="checkbox"/>	Work Phone	+1 (514) 415 3000 x1234	<input type="radio"/>
<input type="checkbox"/>	Mobile Phone	+1 (514) 123-1234	<input type="radio"/>
<input type="checkbox"/>	Work Address	Road, City, Province, Postal Code	<input type="radio"/>

Note: Verify the accepted Telephone Number Format and be aware that the office extension must be between 1 to 6 digits only.

Telephone Number Format

- Country Code (required for non-North American locations; 1-3 digits preceded by a "+" and followed by a space or hyphen).
- U.S. domestic long-distance code (optional; "+1" followed by a space or hyphen).
- Area or city code (required; 2-3 digits).
- Local phone number (required; 7 digits for North American locations, 4-13 digits elsewhere).
- Office extension (optional; letter "x" followed by a 1-6 digit extension).

The separator characters space, hyphen, and open and close parenthesis are allowed where expected.

Examples of valid non-North American numbers:

- +61 29 231 5555
- +33 (01) 56 78 90 12 x200

Examples of valid North American numbers:

- +1 (613) 555 1234
- 613-555-5678 x3429

7. Select a Mutual Authentication Image, enter a Mutual Authentication Phrase, to be known only by you and easy for you to remember then, click the Next button.

* Mutual Authentication Image:



* Mutual Authentication Phrase:

This is my secret phrase ×

Next

Copyright © 2013 Entrust

- In this section, you must select and answer 5 predefined questions from the drop down menus. This will provide you with an alternate method of authentication by the Self-Service module.

N.B.: for all of your answers, do **NOT** use non-English special characters.
Otherwise, you will need to open an incident to delete & re-create your profile.

Entrust IdentityGuard Self-Service

✓ Your personal information has been successfully saved!

Questions & Answers

You must answer 5 predefined questions.

Predefined Questions

Predefined Question 1:

What was the first name of your childhood best friend?

Answer:

Bob

Predefined Question 2:

What is your all-time favorite sports team?

Answer:

The Toronto Maple Leafs

Predefined Question 3:

What was the manufacturer of your first car?

Answer:

Ford

Predefined Question 4:

What city where you born in?

Answer:

Montreal

Predefined Question 5:

What color was your first car?

Answer:


Blue

Next

Click the Next button to continue to the next step.

9. On this step, before clicking on the Yes button, ensure that your Soft Token is opened.
Refer to the next section before proceeding.

Entrust IdentityGuard Self-Service

 Your questions and answers have been successfully saved!

Soft Token

You have been selected to use a soft token for second-factor authentication.

Have you downloaded and installed the Entrust IdentityGuard Mobile application onto your mobile device, or the Entrust IdentityGuard Soft Token application onto your computer?

☒ Yes ☐ No

Not sure what to do?

Answer **Yes** if you've successfully downloaded and installed the Entrust IdentityGuard Mobile or Soft Token application. After answering Yes, you will be prompted to set up a soft token.

Answer **No** if:

- You have **not** downloaded and installed the Entrust IdentityGuard Mobile or Soft Token application yet.
- You don't have a mobile device or computer that can support the application.
- Your attempts to download and install the Entrust IdentityGuard Mobile or Soft Token application have repeatedly failed.
- You are unclear about what to do.

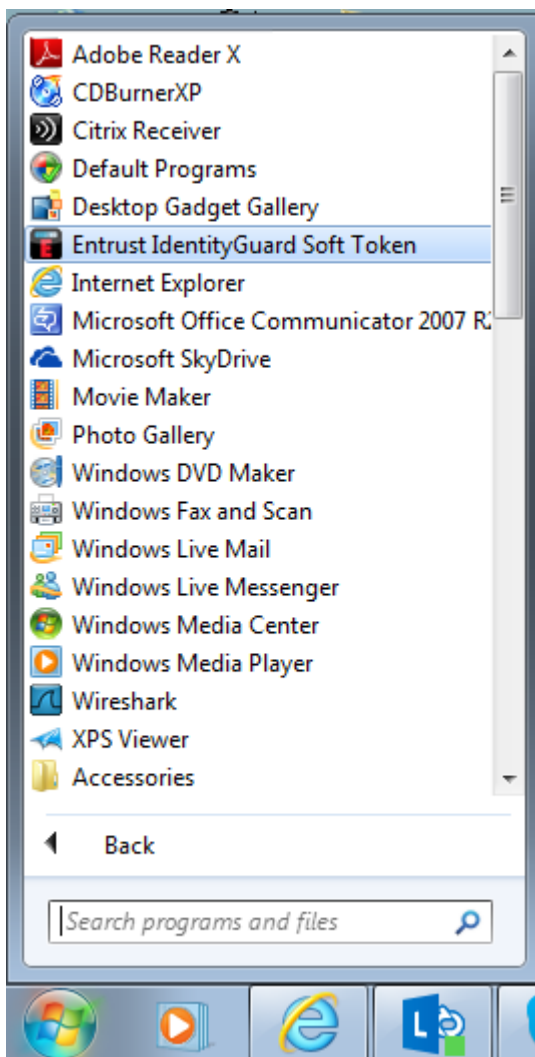
Copyright © 2013 Entrust

4 Activation

This section describes the activation of the Entrust IdentityGuard Soft Token. Before proceeding, ensure that your Soft Token is opened.

If you installed the Entrust IdentityGuard Soft Token on a mobile device, skip this section and go to: **Appendix B - Mobile Installation.**

1. Open the Entrust IdentityGuard Soft Token.
Click: *Start/All Programs* and select *Entrust IdentityGuard Soft Token*.



2. Leave the Address field blank.
 - Enter a name that will describe this Identity (i.e.: Your FirstName)
 - Enter the Serial Number
 - Enter the Activation Code as displayed

Entrust IdentityGuard Self-Service

Entrust IdentityGuard Mobile or Soft Token Identity

Enter the following information into the Identity.

Identity Provider

Address:
<Leave This Field Empty>

Name:
<XXXXXXXXXXXX>

Soft Token

Serial Number:
XXXXXXXX

Activation Code:
XXXXXXXXXXXX

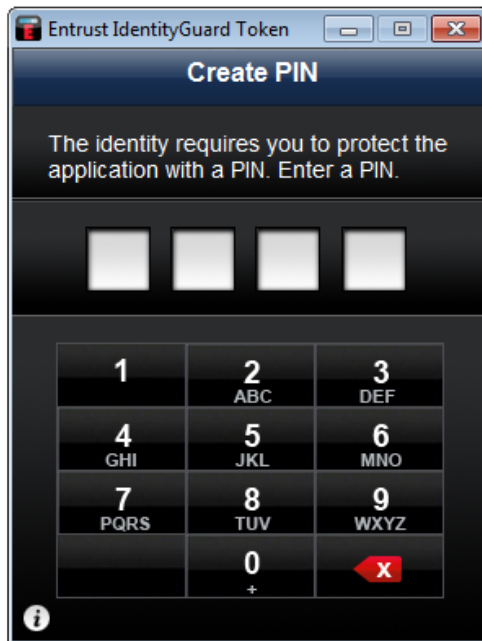
Once you have saved the Identity, return here and click Next.

Not sure what to do?

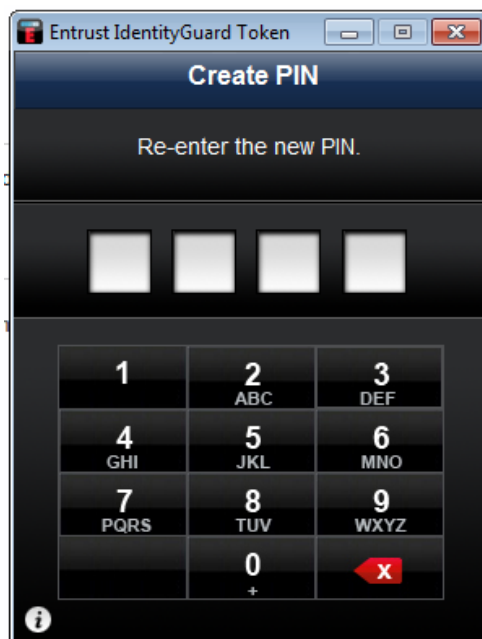
- On your mobile device, open Entrust IdentityGuard Mobile, or, on your computer, open Entrust IdentityGuard Soft Token. Enter your PIN if prompted.
- Select **Add New Identity** if required.
- Leave the Identity Provider Address empty and choose a name for your Identity.
- Enter the Serial Number and Activation Code for your soft token. Select **Save**.
- If prompted, enter a PIN to protect your Identity.
- If you can't continue for any reason, return to this page and click **Cancel**.

Copyright © 2013 Entrust

3. Create a Personal Identification Number (PIN).



4. Confirm the PIN by re-entering it.



5. Enter the Registration Code displayed in the Registration Code field of the Entrust Identity-Guard Self-Service window and click the Next button.

N.B.: This Registration Code will only be displayed once !

The screenshot shows the 'Entrust IdentityGuard Self-Service' web interface. The main heading is 'Entrust IdentityGuard Mobile or Soft Token Registration Code'. Below this, it says 'Complete the activation of your soft token by entering the registration code displayed by the application.' There is a text input field labeled '* Registration Code:' with 'Next' and 'Cancel' buttons below it. A 'Not sure what to do?' section contains two bullet points: 'If the soft token activation information you entered is still being processed' and 'If you don't know what your registration code is, click Cancel.' Overlaid on the right is a mobile app window titled 'Entrust IdentityGuard Token' with a sub-header 'Add Identity'. It contains the instruction 'Enter the registration code into the Self-Service web page, or give it to your help-desk to complete adding the Identity'. Below this is a 'Registration Code' field displaying '22915-26958' in red. At the bottom of the app window is a 'Done' button and the text 'Powered by Entrust'.

6. A Personal Verification Number (PVN), an 8 digit number, will be forwarded to you by email from address: cgientig02@mail.cgimss.com after you click the Next button.

Please keep in mind: you will need to enter this **temporary** PVN to initiate a VPN connection. For more information on how to authenticate via VPN, please refer to the Appendix below.

Entrust IdentityGuard Self-Service

✓ The registration code you provided has been accepted and your soft token activated.

Additional Authentication Types

Soft Token

You have successfully activated the soft token with serial number 62231-41018. You can start using this soft token for second-factor authentication right away!

Personal Verification Number

You will be required to use a Personal Verification Number (PVN) for the following reason:

- Authenticating with your soft token.

Please choose one of your email accounts to have your PVN delivered to you:

▼

You will be required to change the value of your PVN when you first use it.

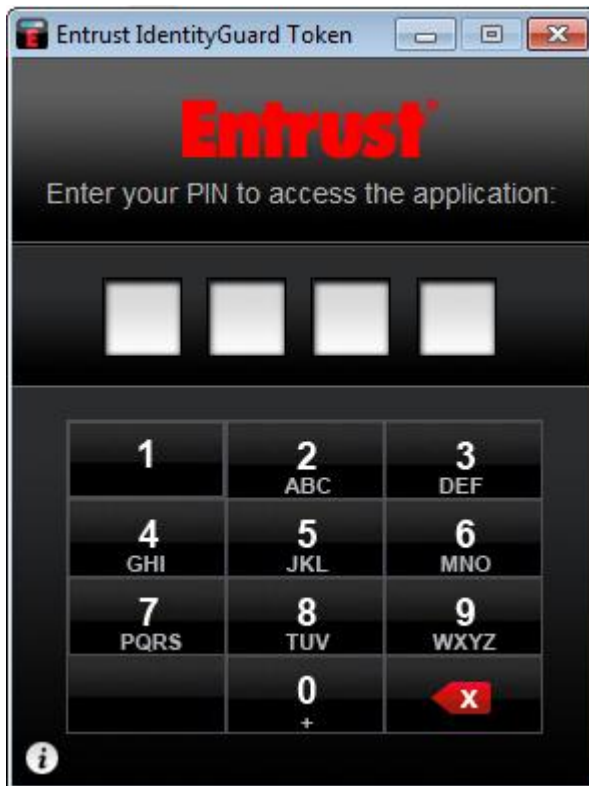
Next

Copyright © 2013 Entrust

After clicking the Next button, the Entrust Identity-Guard Soft Token is activated and can be utilized.

7. Open the Entrust IdentityGuard Soft Token.

- Click: Start/All Programs and select Entrust IdentityGuard Soft Token.
- Enter your 4 digit PIN.



8. A Security Code will be generated for you and will be updated every 30 seconds.



If you require creating more Identities (profiles), click on the Identities button and follow steps 2 to 6 of this section.

5 FAQ

1. **Is there a Self-Service website for my Entrust soft-token/hard token ?**

- Once you registered successfully, you can manage your profile/token thru this site:

<https://cgientself02.ent.cginet:8445/IdentityGuardSelfService>

2. **What options are available to me on the Entrust Self-Service site ?**

The options are:

- I'd like to update my personal information.
- I'd like to change my question and answer pairings.
- I've forgotten my Personal Verification Number (PVN).
- I'd like to get an unlock code since my CGI Enterprise Two-Factors Authentication Mobile OTP or Desktop Soft Token application is locked.
- I'd like to change the name associated with my soft token.
- I'd like to recreate my soft token since I deleted its Identity from my device.
- I'd like to reinstall the CGI Enterprise Two-Factors Authentication Mobile OTP or Desktop Soft Token application on my current device or a new device.

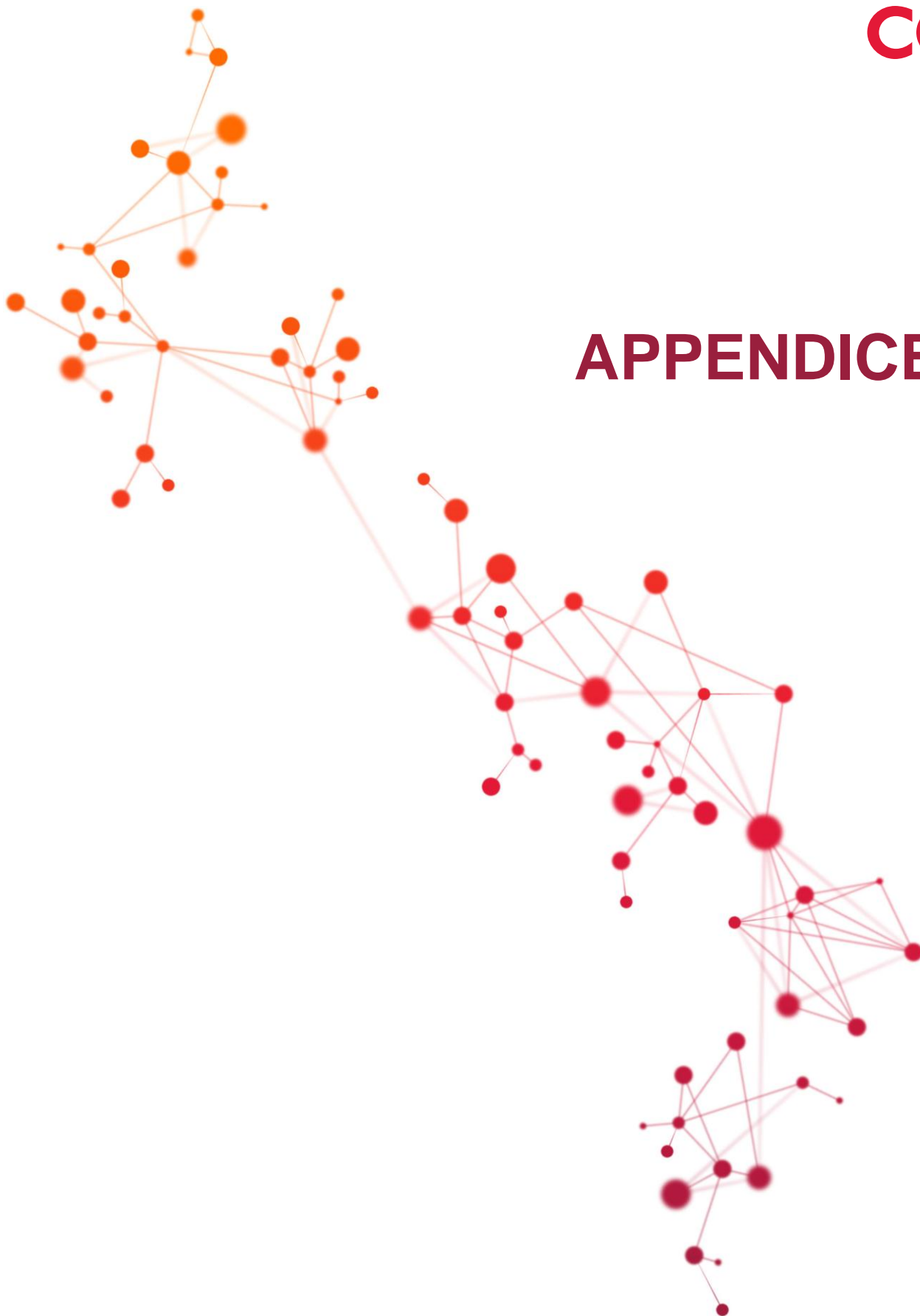
For any options that you select, you just need to follow the on-screen instructions to complete the process.

3. **How do I change my Personal Verification Number (PVN) ?**

- Our suggestion is to change your PVN thru the Entrust Self-Serve site & select the option: I've forgotten my Personal Verification Number (PVN).

You just need to follow the on-screen instructions to complete the process.

APPENDICES



Appendix A – Hardware Token

The Entrust hardware tokens are provided to members on a limited basis (i.e.: specific project, client technical requirement (banking), time-restricted access, etc.).

When you will receive your Entrust hardware token, you will also receive some instructions from the Authentication team to contact them. The Authentication team will be completing the following steps with you:

1. Registration of your user profile with your hardware token
2. Activation of your user profile with your hardware token
3. Synchronization of the hardware token with Entrust authentication server
4. Creation of your PVN (Personal Verification Number)
5. Test VPN Authentication

Once all these steps are completed with the Authentication team, your hardware token will be active & ready to use.

FAQ for your hardware token:

How do I turn ON the hardware token and generate a token number ?

- Hold the button down until the status bar fills the display with dashes. Release the button as soon as the token number appears. You will have about 30 seconds to use these numbers before the token turns itself OFF and the number disappears.



How do I turn the token off when a token number is displayed ?

- The token will turn off after 30 seconds of inactivity. You can quickly press and release the button to turn the token off, but the preferred method is just to wait 30 seconds.

My token is displaying rotating information instead of a token number.

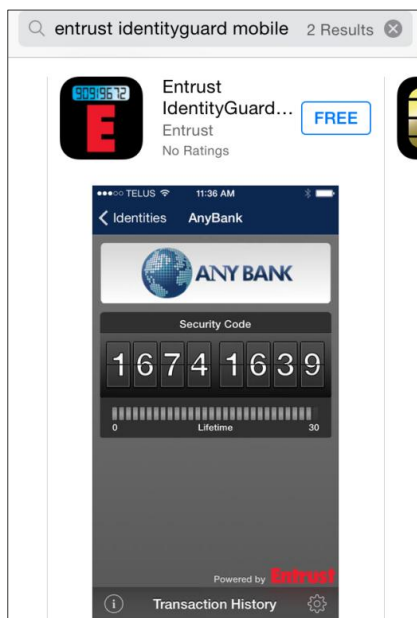
- This can happen if you hold the button down for approximately 2 seconds when a token number is displayed. Your token will turn off after 30 seconds. You will be able to generate a token number the next time you turn the token on.

Appendix B - Mobile Installation

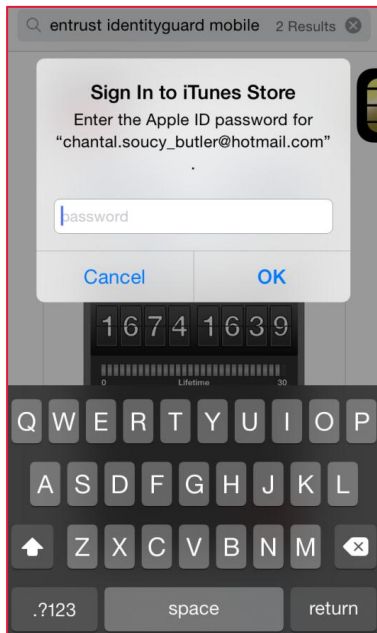
This mobile installation is based on an iPhone installation, but you can use this process since the installation process is similar for the following mobile devices:

- Win Mobile 8.x from Windows Phone Store (Entrust OTP)
- Android - Google Play (Entrust IdentityGuard Mobile)
- Blackberry - Blackberry World
 - a. Entrust IdentityGuard Mobile
 - b. Entrust IdentityGuard OTP for BlackBerry 10
- Nokia Symbian OS

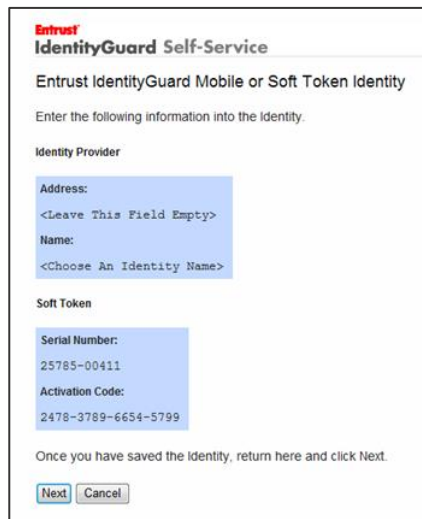
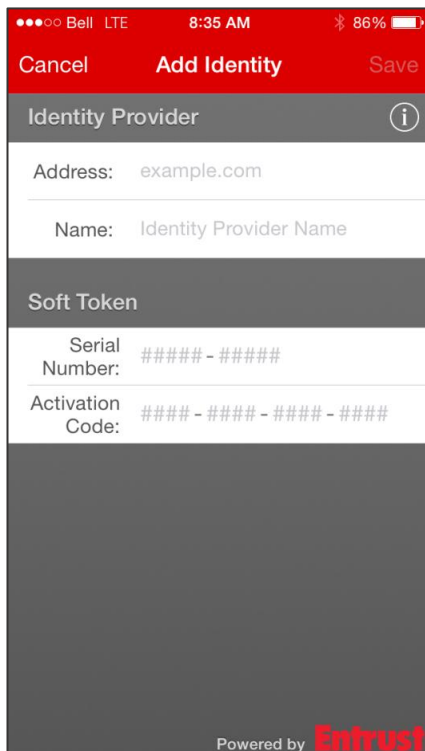
1. From the Apple App Store search for the Entrust IdentityGuard Mobile application and activate the download process by clicking “Free” then “Install”.



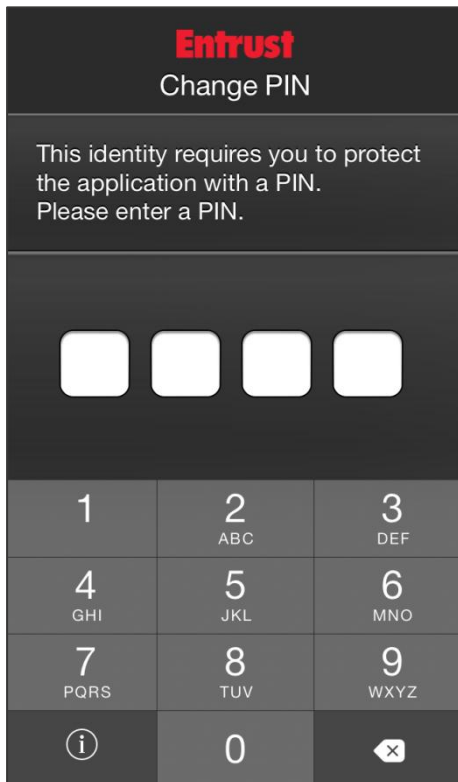
2. Enter your Apple ID password.



3. Once the application is installed, enter your **Name** then the **Serial Number** and **Activation Code** generated during the Entrust Registration process then save.



4. To protect the process of creating an Identity, you are required to set a PIN number.



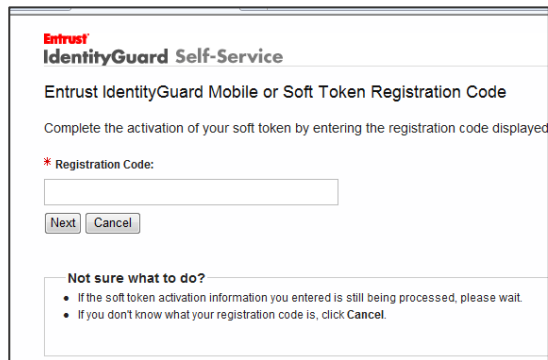
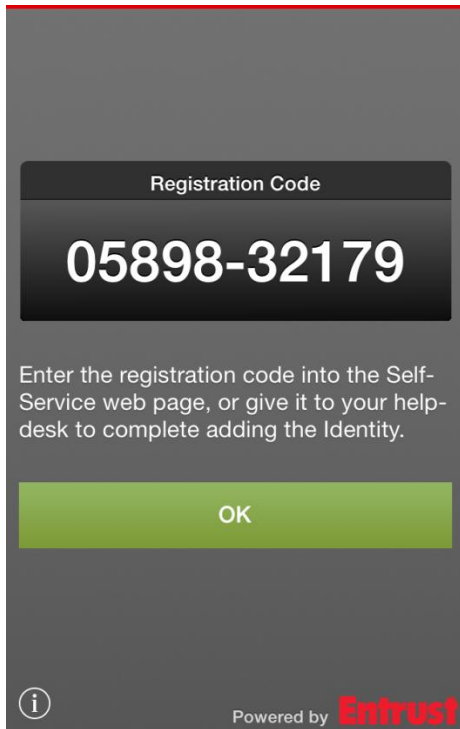
Entrust
Change PIN

This identity requires you to protect the application with a PIN.
Please enter a PIN.

Four white square input fields for the PIN.

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
(i)	0	⬅ X

5. Once your password is selected and confirmed, a Registration Code will be generated and is to be entered in the Registration Code field of the Entrust Identity-Guard Self-Service window. Once entered select OK to complete the installation.



6. A Personal Verification Number (PVN) will be forwarded to you by email after you click the Next button within the Entrust Identity-Guard Self-Serve window. This PVN will be required to start a VPN session.

Entrust IdentityGuard Self-Service

✓ The registration code you provided has been accepted and your soft token activated.

Additional Authentication Types

Soft Token

You have successfully activated the soft token with serial number 62231-41018. You can start using this soft token for second-factor authentication right away!

Personal Verification Number

You will be required to use a Personal Verification Number (PVN) for the following reason:

- Authenticating with your soft token.

Please choose one of your email accounts to have your PVN delivered to you:

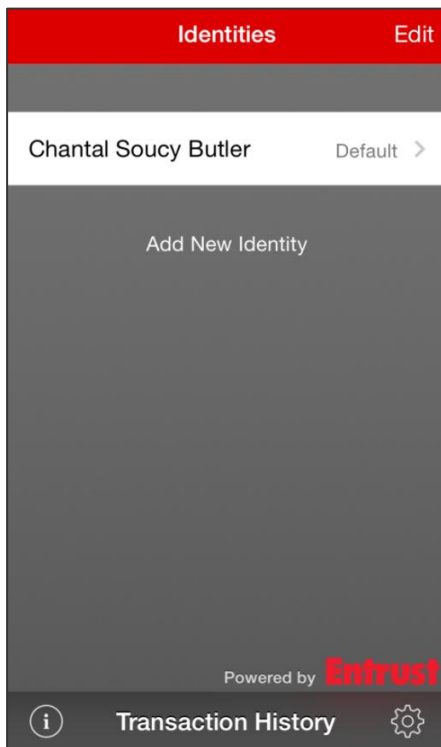
▼

You will be required to change the value of your PVN when you first use it.

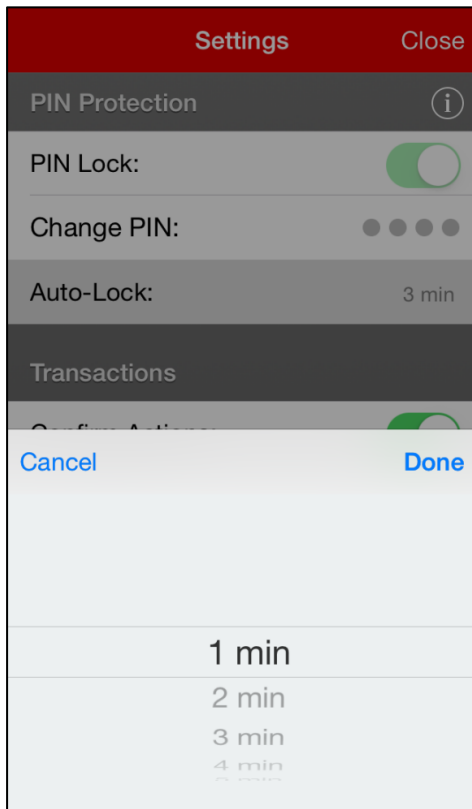
Copyright © 2013 Entrust

NOTE – After clicking the Next button, the Entrust Identity-Guard Soft Token is activated and can be utilized.

7. To modify security settings, click the “cog wheel” icon in the bottom right corner.



8. PIN Lock is to remain active. Auto-Lock setting should be changed to 1min.



Once this step is completed, proceed to the specific Appendix below which is associated to the type of VPN/Web Gateway for which you want to authenticate.

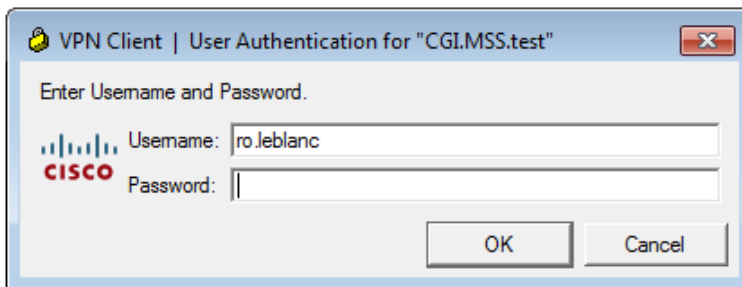
Appendix C - Cisco VPN

The Personal Verification Number (PVN), an 8 digit number forwarded to you by email from address: cgientig02@mail.cgimss.com is required to proceed.

1. Start the Entrust IdentityGuard Soft Token application.
2. Start Cisco VPN and initiate a connection using your required profile.
 - Enter your Username: first part of your CGI email in the format: *firstname.lastname* (The first part of your email address without the @cgi.com).
 - Enter your Password: the 8 numeric digits PVN (email from cgientig02@mail.cgimss.com) + the 8 numeric digits generated by the Soft Token.
 - Click OK.

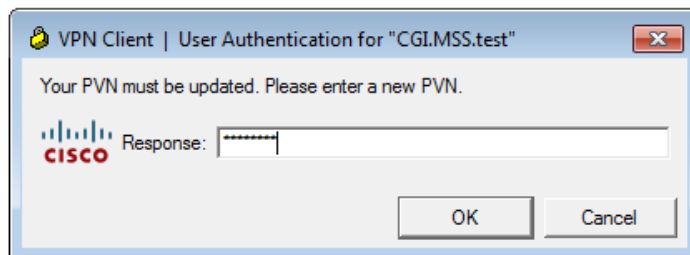
N.B.: If you authenticate to the following VPN host: **rnasMTLinternal.ent.cginet**

You must use your full username (example: john.doe@cgi.multi.rsa.inside) for a successful authentication through Entrust.



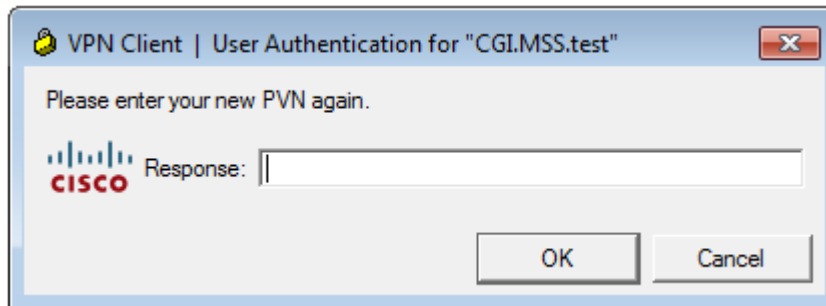
3. Enter a new PVN of your selection (**MUST be 8 numeric digits only**).

- Click OK.

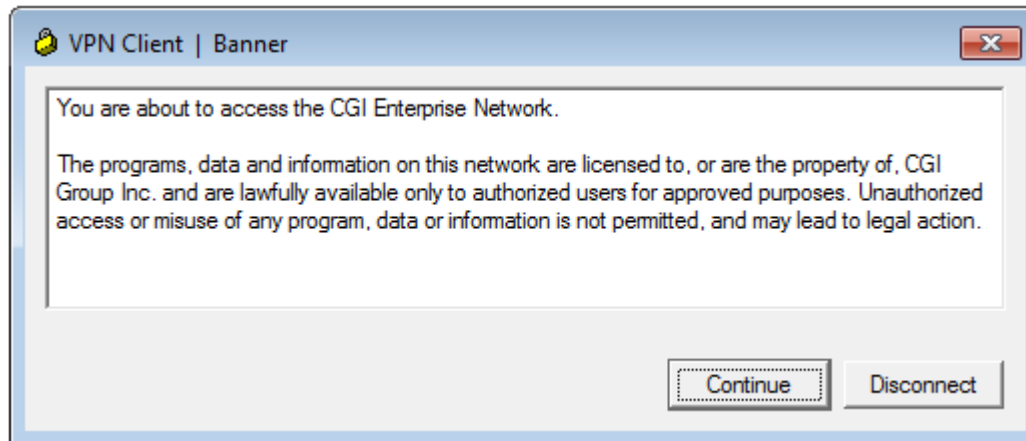


4. Re-enter your newly created PVN.

- Click OK.



5. Your Cisco VPN connection will then be initiated.



- Click the Continue button.

Appendix D – ex-Logica Web Portal

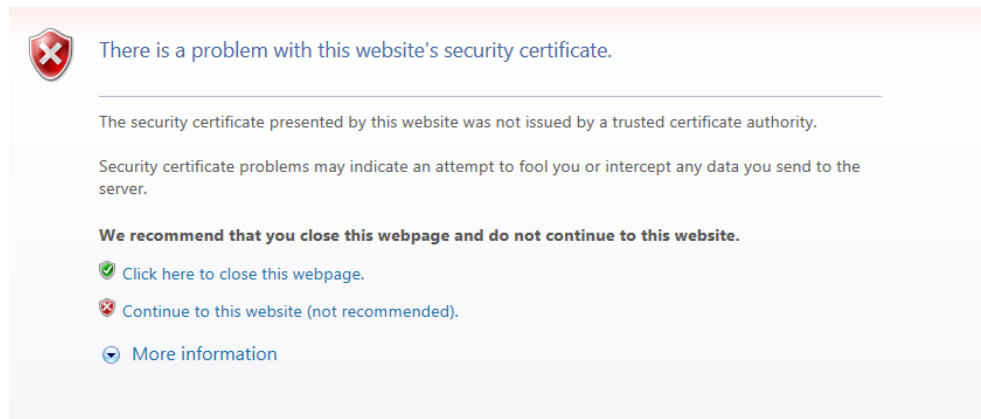
The Personal Verification Number (PVN), an 8 digit number forwarded to you by email from address: cgientig02@mail.cgimss.com is required to proceed.

N.B.: You must follow all the steps in sequence for your activation & authentication to be successful.

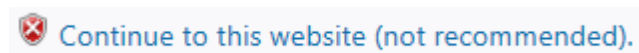
1. Start the Entrust IdentityGuard Soft Token application.
2. Access your usual Juniper Remote Access Gateway via the 1 of the following webpage (NOT via Network Connect or Junos Pulse):

<https://gateway2.logica.com>
<https://gateway3.logica.com>
<https://gateway5.logica.com>
<https://gateway6.logica.com>
<https://augateway.logica.com>
<https://sydgateway.logica.com>

3. if you see the following screen (if not, skip to step 4)



Click/select:



Once you reached the site, you will see the following:



Authorised users only
CGI Gateway 2

Username
 Password/Passcode
 Realm

Please click the "Useful Information" button if you have problems logging in or would like basic instructions.

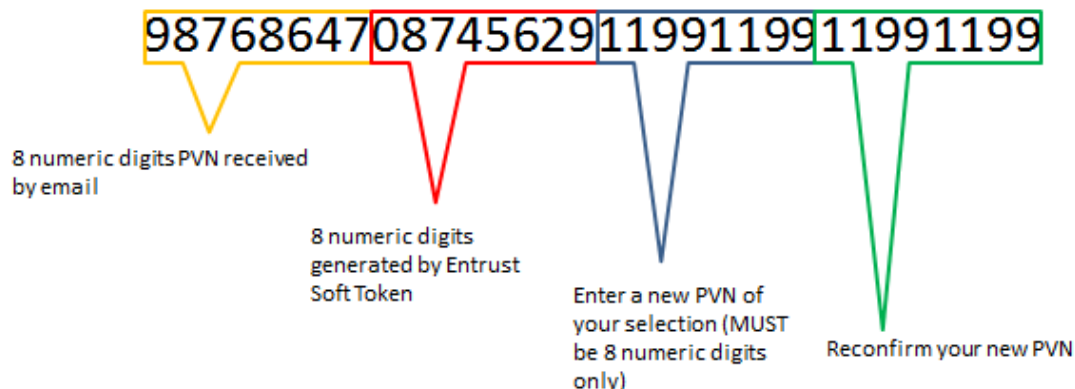
The URL to an alternative gateway is <https://gateway3.logica.com>

You may access the web version of Office Communicator directly, without having to login to the Gateway, by accessing the url <https://uccwa.logica.com>

The provisions of the United Kingdom's Computer Misuse Act 1990 makes attempting to gain unauthorized access to computer systems a criminal offence punishable by imprisonment.

4. Enter your Username; first part of your CGI email in the format:
firstname.lastname (The first part of your email address without the @cgi.com).
5. Under the Password/Passcode line:
 - Enter the 8 numeric digits PVN (email from cgientig02@mail.cgimss.com)
 - Then followed by the 8 numeric digits generated by the Soft Token
 - Then followed by a new PVN of your selection (**MUST be 8 numeric digits only**)
 - Then re-enter the new PVN you selected in previous step to confirm

To illustrate the steps above, the string of numeric digits can look like this:

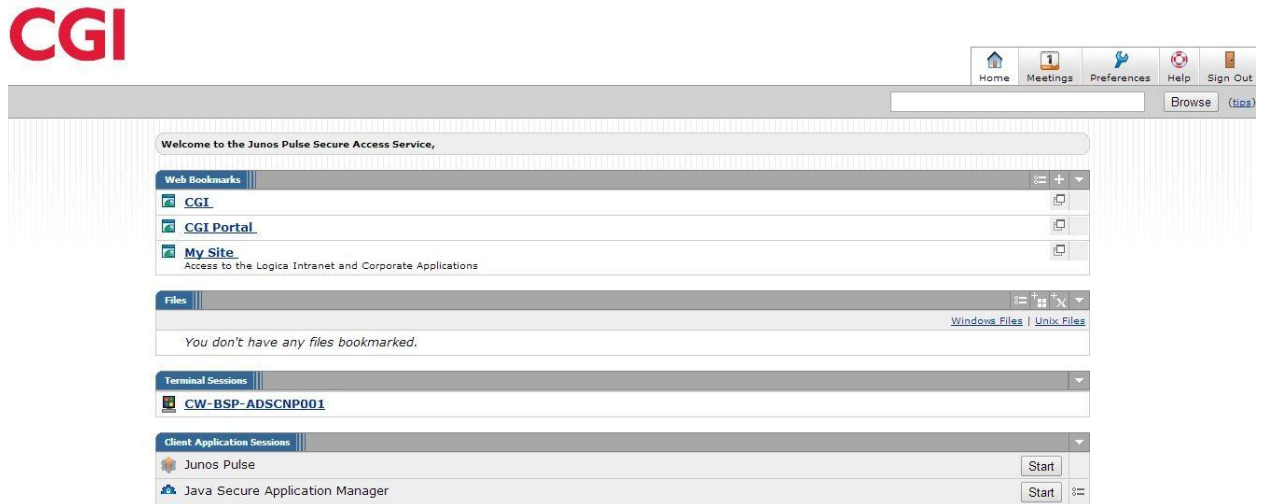


N.B.: This long string of numeric digits is required, since you are creating your new PVN. For future VPN authentication, you will need to enter the PVN (8 numeric digits you created) + the 8 numeric digits generated by the Soft Token only.

6. Under Realm, select Entrust in the drop-down menu.

- Then click the Sign In button.

7. If you authenticate successfully, you will see the following site.

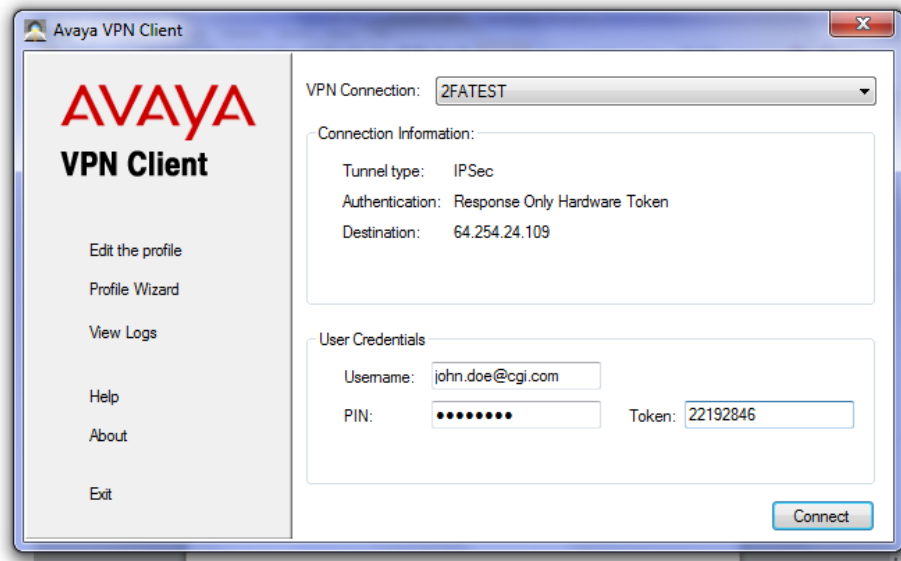


If you did authenticate successfully, please disconnect & reconnect thru your regular VPN connection, by entering your PVN (8 numeric digits you created) + the 8 numeric digits generated by the Soft/Hardware Token only

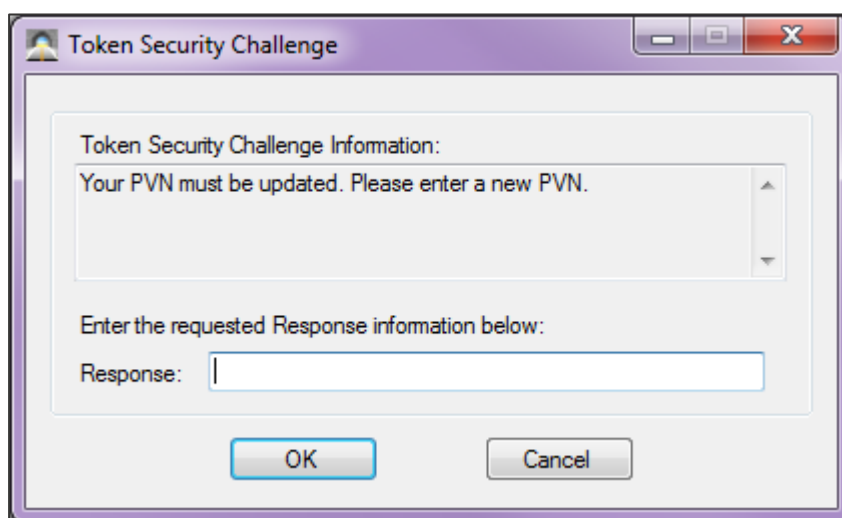
if you cannot authenticate successfully, please refer to section 1.2 Assistance.

Appendix E - Avaya VPN Client Connection

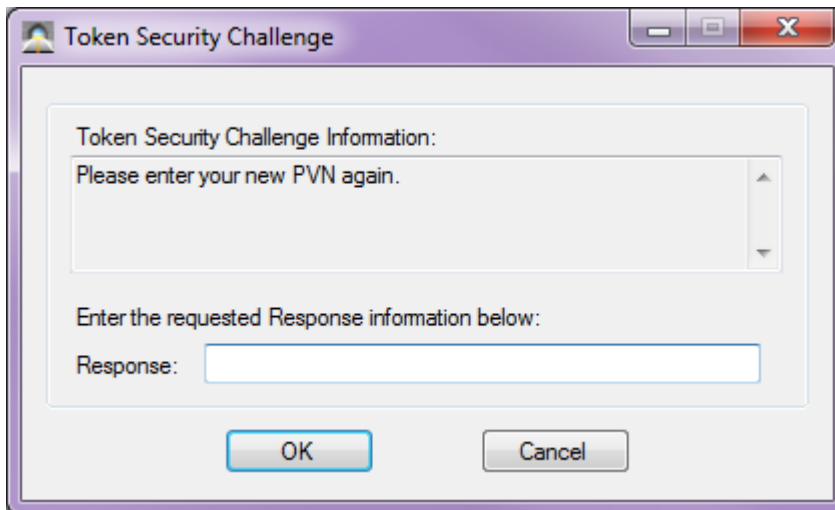
1. Select the appropriate VPN Connection from the drop list. Once selected, enter your username (be sure to include @cgi.com), your **Personal Verification Number** in the PIN field, and a **Security Code** response from your Soft-Token then click "Connect"



2. From the Token Security Challenge screen, select a new **Personal Verification Number** that **MUST be 8 numeric digits only** and then click OK.



3. Reenter your new **Personal Verification Number** to complete the VPN authentication process then click OK.



Revision History

Version	Date	Author	Description
0.1	5/20/2014	Roger LeBlanc	Initial document.
0.2	5/20/2014	Roger LeBlanc	Page 1 section 1.2 and page 15.
0.3	5/20/2014	Roger LeBlanc	Added iPhone directives on page 14 and in Appendix - B (step 6).
0.4	5/21/2014	Roger LeBlanc	PVN password update in the AVAYA VPN page 24 of Appendix - A by Chantal R. Soucy-Butler.
0.5	5/21/2014	Roger LeBlanc	Added Appendix - C Cisco VPN.
0.6	5/22/2014	Roger LeBlanc	Updated User Name format in Section 3, Page 8 and Step 3 in Appendix - C Cisco VPN, page 31, step 2.
1.0	5/22/2014	Roger LeBlanc	Client version.
1.1	5/23/2014	Roger LeBlanc	Added connection to CGINet or SERA Connect as a prerequisite in Section 1.1 on Page 1.
1.2	5/23/2014	Roger LeBlanc	Added warning for CGI members working outside of a CGI site in Section 2 Page 2 and in Section 3 Page 8.
1.3	6/5/2014	Roger LeBlanc	Removed the user questions to answer procedure in the Self-Served section of page 12.
1.4	6/12/2014	Roger LeBlanc	Changed section 6 on page 10 to prevent default selection.
1.5	6/12/2014	Eric Bélair	Changed section 6 on page 10 to prevent default selection.
1.6	07/04/2014	Sylvie Maher	Changed on Appendix A and C to prevent double authentication.
1.7	08/22/2014	Eric Bélair	Update of Appendix C – VPN Cisco, item 2.
1.8	08/29/2014	Eric Bélair	Update of Section 4, item 6 & Appendix C – VPN Cisco, items 2 & 3.
1.9	09/11/2014	Eric Bélair	Review & modifications to documentation.
2.0	09/11/2014	Eric Bélair	Added Appendix C – ex-Logica Web Portal.
2.1	10/06/2014	Eric Bélair	Minor modifications to documentation, also added Appendix A – Hardware Token
2.2	10/07/2014	Rob Davies & Richard Bedford	Modifications for legacy Logica.
2.3	10/07/2014	Rob Davies	Added additional mobile phone install information and compatibility
2.4	10/13/2014	Eric Bélair, Rob Davies & Richard Bedford	Modifications to documentation based on CGI member's feedback.