# KB article (How to Login using Cisco AnyConnect VPN Start Before Logon (SBL) or GINA Module) KB0013143

# KB Article: <https://ucf.service-now.com/ucfit?id=kb_article&sysparm_article=KB0013143&sys_kb_id=b5dd2615db63109003f806d1ca961935&spa=1>

Cisco AnyConnect VPN has a new feature called Start Before Login (SBL), also known as the “GINA” Module. This feature will allow you to login to the VPN before signing into your workstation (e.g., before it displays the desktop on your Domain-Joined Windows 10 device). Use this feature when:

* + You are remote (I.e., not on campus using a campus network connection) and have never previously signed into a domain-joined workstation.
  + You reset your password while not signed on to a campus network connection
  + When you wish to have updated workstation policies applied while not using a campus network connection.

|  |
| --- |
| **Please Note:** The SBL/GINA Module and the Cisco AnyConnect Client Agent versions need to match exactly for it to function properly. Please ensure the clean installation of both modules as a primary Troubleshooting step. |

**Install Cisco AnyConnect Secure Mobility Client with SBL/Gina Enabled**

The best way to get the Start Before Login (SBL) software installed is from **Software Center**. The application will automatically install or upgrade existing Cisco AnyConnect components to the latest available version.

From a computer issued by UCF, you can access the **Software Center** (a catalog of applications you can install yourself) by clicking the start menu and typing in “software center”. You can search for the Cisco AnyConnect Client from **Software Center.**

* + Opened the **Software Center** by clicking the windows start menu and search for “**Software Center”,** in the Software Center Applicationsearch forthe Cisco AnyConnect and click on install to install the software (see picture below).
  + **NOTE:** If you do not have access to the application in **Software Center**, please use the following information to contact the UCF Service Desk for assistance.

UCF Service Desk:

* Phone: 407.823.5117
* Email: [itsupport@ucf.edu](mailto:itsupport@ucf.edu)
* Hours: Monday to Friday, 7 a.m. to 10 p.m.
* Website: it.ucf.edu

Graphical user interface, text

Description automatically generatedOpen Software Center and search using the keywords “Cisco” or “AnyConnect” and click Install

**Please Note:** The Software will need to be made available in the Software Center to a particular zone/area before it will be visible in Software Center. Please contact the Endpoint Engineering Services (UCFTeam-UCFIT-EndpointEngineeringServices@groups.ucf.edu) for assistance on deployments if needed.

### **How to Use Cisco AnyConnect Mobility Client “Start Before Logon” feature from the User’s login screen:**

* + Enter username: **Your NID**
  + Enter password: **Your NID Password**
  + **The Multifactor Authentication (MFA) challenge will be prompted:**
    - **Note:  Only DUO push or Call me is supported.** We recommendusing the **Duo Mobile App** (available from Apple or Google app stores) for the best experience. Please follow the instructions below to get started.
    1. Enroll your mobile device: <https://guide.duo.com/enrollment>
    2. iPhone Device: <https://guide.duo.com/iphone>
    3. Android Device: <https://guide.duo.com/android>

Using the VPN at the **User’s** **login screen** is completely optional. To use the VPN from the User’s login screen please refer to the steps below.

1. Clicking on the new network icon from the User’s login screen appeared to the left of the built-in Windows network status icon as shown in the screenshot below.

Graphical user interface, website

Description automatically generated

1. Enter the VPN URL (**secure.vpn.ucf.edu**) if isn’t prepopulated and click connect

Graphical user interface, website

Description automatically generated

1. Choose “**UCF\_StartBeforeLogon**” from the group dropdown menu and enter your NID username and NID Password and approve your DUO challenge. (**Duo Push is recommended**)

Graphical user interface, application

Description automatically generated

1. Accept **UCF System User Agreement** to be connected to the VPN.

Graphical user interface, text

Description automatically generated

1. Once the VPN connection has been established, Login to the computer with your NID username and password.   
     
    A screenshot of a computer

   Description automatically generated with medium confidence

**Please note: Some workstations or devices have restrictions on which accounts can be utilized to login interactively. Any device capable of running the Cisco AnyConnect client that meets the UCF standards can connect to the UCF Enterprise VPN>**