Logo, company name

Description automatically generated

**Installing GlobalProtect VPN**

# Purpose

The purpose of this documentation is the describe the process in which to install the GlobalProtect VPN client. This client allows users to access the SMC Internal network while away from a company campus or office.

Contents

[Purpose 1](#_Toc107216045)

[Solution/Process Description 2](#_Toc107216046)

[Prerequisites 2](#_Toc107216047)

[*IT Security Request* 2](#_Toc107216048)

[*Okta MFA* 2](#_Toc107216049)

[Installing GlobalProtect VPN 4](#_Toc107216050)

[Document Information & Revisions 6](#_Toc107216051)

[**REVISION HISTORY LOG** 6](#_Toc107216052)

[**REVIEW / COMMENTS** 6](#_Toc107216053)

# Solution/Process Description

## Prerequisites

There are two prerequisites that must be completed prior to gaining access to the VPN. The prerequisites are as follows:

1. An approved **IT Security Request**
2. **Multi-Factor Authentication** (MFA) enabled within Okta.

### *IT Security Request*

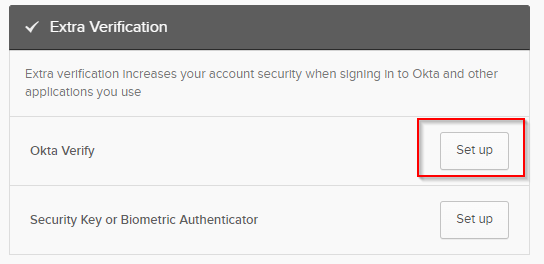
An IT security request can be entered via Lotus Notes. When entering a request for VPN, make sure to choose the “VPN” option. Many of the options are handled by different IT personnel, so in order to expedite your request, always make sure to choose the option that best matches the system you are attempting to gain or change your access to.

Once the Security Request is approved by your manager, an IT ticket will be generated. Additional approval will be sought by the designated IT personnel; after this is granted, the technician/administrator off the application will reach out to you with any applicable instructions or credentials required to access the VPN.

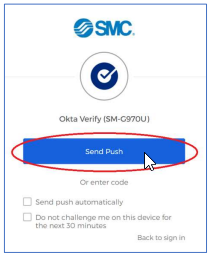
### *Okta MFA*

As of June 2022, Okta MFA is required in order to access the new VPN portal address. Please see the steps below that must be taken to enable Okta MFA:

1. Log in to Okta at the following address: <https://1smc.okta.com/>
2. In the top-right side of the homepage, click your name, then *Settings*
3. Within the *Extra Verification* Section, select *Set up* across from *Okta Verify:*

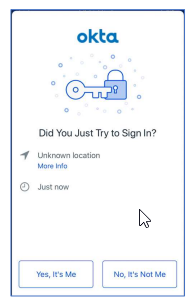


1. At the next screen, click *Setup*
2. Select your device type, either iPhone or Android
3. You will be instructed to download the *Okta Verify* application to your phone – click *Next* once you have done so
4. Follow the instructions on-screen to add your SMC Okta account to your Okta Verify app.
5. From now on, when you log into Okta, you may be prompted for a second factor to prove that it is you logging in. Click *Send Push* to send a notification to your phone:



*(seen after logging in to Okta from a new device)*

1. On your phone, after receiving and opening the push notification, tap *Yes, It’s Me*:



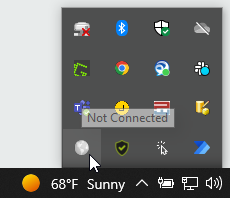
*(seen after opening the notification on an Android phone)*

1. You should now be logged into Okta.

## Installing GlobalProtect VPN

*Note: If you do not have elevated access to your machine, IT will likely request to remote in to your machine to perform these steps for you.*

1. Once the prerequisites have been met, navigate to <https://vpn.1smc.com>
2. Here, log in using your Network/Okta credentials. If you are already logged in to Okta you will likely not get a login screen; you will only be required to enter your username.
3. In the top-right of your screen, select *GlobalProtect Agent*
4. Select the version to download. For most, you will want to install the Windows 64-bit agent
5. Once installed, double-click the client icon to open the client. The client is located in your taskbar (grey globe):



1. Enter **vpn.1smc.com**in the portal address prompt
2. Log in using your network/Okta credentials
3. You will be greeted with an Okta MFA prompt. Complete the MFA
   1. If you are already signed in to Okta, you may not be prompted to complete MFA
4. Once completed, the web browser will prompt you to allow the page to open the Global Protect app.
5. Click *Allow*

GlobalProtect will then connect after a few moments.

The first time you connect to the VPN, the client will likely go through an update process. No actions are required on your part; the update will complete on its own.

If you have used the VPN before, you may remember that you were required to turn it off when you are on-campus. That however is no longer the case. The VPN is now configured to be “always-on.” You will be able to access internal resources whether you are on-campus, at a coffee shop, at home, etc.

# **Document Information & Revisions**

|  |  |
| --- | --- |
|  | |
| **Document Owner** | System Administrator, NA IT Line-of-Business Unit |
| **Effective Date** | June 27, 2022 |
| **Authored By** | Austin Herschberger |
| **Reviewed By** | IT Manager |
| **Review Schedule** | Annual |

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISION HISTORY LOG** | | | |
| **Version Number** | **Date** | **Author** | **Summary of Change** |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **REVIEW / COMMENTS** | | |
| **Date Reviewed** | **Reviewed By** | **Approval or Suggested Comments** |
| 06/27/2022 | Sebastian Rubio | Document Approved |
|  |  |  |
|  |  |  |
|  |  |  |