Coronavirus Update 3/17/20

Office of the President <OfficeOfThePresident@USF.EDU>
Tue 3/17/2020 4:46 PM
USF_COMMUNICATION_FOR_EMPLOYEES@LISTSERV.USF.EDU

Dear USF community,

There is nothing more important than the health and wellness of our community as we work to respond to the rapidly evolving COVID-19 (coronavirus) pandemic. It is this belief that guides our every decision, utilizing the latest guidance of our governmental and health leaders.

Today, Florida Gov. Ron DeSantis and the Board of Governors directed our state universities, including the University of South Florida, to continue providing remote instruction for the duration of the spring semester. **This means that, if able, students should make plans to remain off campus until at least May 7**. USF employees (faculty, staff and OPS) who are able to work remotely should continue to do so until at least April 6, however USF leadership will continue to monitor the situation to provide updated guidance, as needed.

Student Health Services and USF Health clinical operations will continue as usual, unless otherwise noted.

Residential students will receive separate guidance shortly.

Commencement is a vital element of our university community and an important milestone in the lives of our students and their families. Per Board of Governors direction, the spring 2020 commencement scheduled for May is postponed until further notice. We understand this is very disappointing to our graduates and their families. This is not a decision we take lightly, and we are working diligently with student leaders to develop creative alternative solutions to give our graduates the recognition they have rightly earned, including the possibility of expanding August ceremonies to include spring graduates. More details will be provided as soon as possible.

USF is dedicated to the success of our students. We are also committed to the availability of high-quality online course delivery throughout the summer to ensure academic continuity.

Remote instructional resources

All classes and necessary support functions will continue remotely through the spring semester. USF has developed a myriad of tools, technologies, training and other resources to assist in this transition.

We have now updated both our ***USF Toolkit for Instructional Continuity*** for faculty and our ***USF Toolkit for Continuity of Student Support*** to facilitate remote student access to important resources and services, such as counseling, advising, tutoring and other needs.

Importantly, beginning next week, all students will have access to Microsoft Teams and Office 365, providing an additional resource for collaboration with faculty and student peers. A separate communication will follow shortly with more details from USF IT.

Campus events and social gatherings

Per federal guidance, individuals should limit any gatherings of more than 10 people for at least the next two weeks. This means that all face-to-face meetings, organizational gatherings or other social events of this size should be canceled or conducted virtually.
All events on campus, at other USF instructional sites or off campus are postponed or canceled until further notice.

USF Libraries will also be closed to all visitors (USF faculty, staff, students and the general public) until further notice. Virtual library services will continue for students and faculty.

USF employee guidance

Per guidance provided March 15, any USF employees (faculty, staff and OPS) who can work remotely should do so until at least April 6. USF leadership will continue to monitor the situation to provide updated guidance, as needed.

Employees must work with their supervisors to develop a plan that allows them to meet deliverables and maintain communication, productivity and efficiency.
Employees whose job duties do not allow for remote work or who do not have necessary IT resources should talk to their supervisors about designing on- or off-campus work arrangements that will still fulfill their obligations without exposing undue risks to their own health and safety or that of the campus community.

Healthcare-delivery employees, including USF Health clinical staff and Student Health Services staff, are expected to report to work as usual unless they receive separate guidance from their supervisors.

For guidance with IT resources visit **www.usf.edu/it-remote-resources**.

Please contact USF Human Resources at 813-974-2970 or **Employee-Relations@usf.edu** with additional questions.

Faculty and staff who are concerned about their health should contact Dr. Lynette Menezes in USF Health at **healthglobal@usf.edu**.

Health guidance

Please continue to practice social distancing and good hygiene. Wash your hands frequently with soap and water for at least 20 seconds, especially after going to the bathroom, before eating, and after blowing your nose, coughing or sneezing. If soap and water are not available, use an alcohol-based hand sanitizer with at least 60% alcohol.

Students who need guidance or medical assistance should contact Student Health Services:

- Tampa Student Health Services (SHS100) at 813-974-2331
- St. Petersburg Wellness Center (SLC 2200) at 727-873-4422
- Sarasota-Manatee Counseling and Wellness Center (5805 Bay Shore Rd.) at 941-487-4254

The health and wellness of the USF community is always our first priority. We deeply appreciate your adaptability as we work to respond to this rapidly evolving pandemic.
Please continue to refer to **www.usf.edu/coronavirus** for the latest information and resources.

Thank you,

Steve Currall
President and Professor

Approving a Telecommuting Arrangement

Vice Presidents/Provost may authorize telecommuting arrangements for employees under their direction that are in the best interests of the university, including authorizing the use of equipment and/or services owned or paid for by the university as well as telecommunications. This authority may be delegated to deans and directors, except they may not approve their own telecommuting arrangements.

Procedures should be developed for each vice-presidential area with respect to the approval of telecommuting arrangements. Such procedures must be in compliance with all applicable laws and university regulations, policies, and procedures. At a minimum, eligibility for telecommuting should be based on an evaluation of suitability of the job and likelihood of success with such an arrangement. Because of the potential implication of wage and hours laws and the monitoring, restrictions, and record keeping associated with hours worked by non-exempt employees, telecommuting agreements are typically limited to exempt (Administration) employees. Additional guidance for developing procedures and approving telecommuting arrangements can be provided by the Division of Human Resources (“DHR”). DHR must approve telecommuting agreements involving non-exempt employees.

Engaging in a Telecommuting Arrangement

Each employee entering into a telecommuting arrangement, for telecommuting on other than an incidental or occasional basis or for which the university will provide equipment and/or services, will have a written agreement with the university. The Telecommuting Agreement form should address the terms and conditions of the telecommuting arrangement, including, but not limited to, duration, work hours, location, description of equipment and/or services the university and/or employee will provide, expenses to be paid by the university and/or employee, and how work will be evaluated.

Employees working at a telecommuting site are obligated to comply with all applicable laws and university regulations, policies, and procedures.

The designated telecommuting site is to be maintained in a safe condition, free from any hazards to the employee and any danger to university property located at the site, to the extent possible. However, the university is not liable for damages to the employee's property resulting from the telecommuting arrangement.

While working at the telecommuting site, it is the employee’s responsibility to properly safeguard documents/records from loss, damage, or unauthorized access and to prevent unauthorized access to any sensitive or confidential information and data via computer or other telecommunications.

Employees, while engaged in work at the telecommuting site, are covered by workers' compensation. As such, employees must authorize appropriate officials access to the telecommuting site to perform safety inspections and/or investigate a workers' compensation claim.

When the designated telecommuting site is the home, employees should schedule work during a time when interruptions can be kept to a minimum. Employees should not be responsible for care-giving for children, parents, or others during their scheduled hours of work.

The university will not be responsible for operating, maintenance, or other incidental costs associated with use of the employee's home as the designated telecommuting site.

Employees who have been approved for a telecommuting arrangement are responsible for determining any income tax implications of maintaining a home office. The university will not provide any tax guidance nor assume any additional tax liabilities.

A telecommuting agreement may be terminated in writing at any time, either by the employee or by management, when it has been determined that it is not in the university's best interest for the telecommuting arrangement to continue. Also, failure of an employee to comply with the provisions and conditions of the agreement may result in termination of the agreement and telecommuting arrangement and/or appropriate disciplinary action.

Equipment and/or Services Owned or Paid for by the University

Generally, equipment and/or services owned or paid for by the university will not be provided for an employee when the telecommuting arrangement is authorized solely for the convenience of the employee.

When telecommuting arrangements warrant the expenditure of university funds for the purchase of equipment or services or the reimbursement of expenses, those expenditures are to be approved prior to being incurred. Approval of such expenditures must be documented in the written agreement addressed above.

Typically, maintenance and service of university-owned equipment used at the telecommuting site will be the responsibility of the university.

When a telecommuting arrangement ends, it is the responsibility of the employee's department to account for any university-owned equipment used at the telecommuting site and to ensure services are terminated that are no longer required.

Provision and use of equipment owned and/or services paid for by the university for a telecommuting arrangement must be in compliance with established procedures as follows:

Requesting/Purchasing Equipment and/or Services

- Telecommunications equipment and/or services - Telephones and related equipment and services are requested through Information Technology by way of a properly executed Request for Communications Services.
- Other equipment and/or services - Computers, printers, fax machines, scanners, computer software, service/maintenance agreements, and other required equipment and services are requested through Purchasing and Property Services. See FIND IT for a link to COMPASS for detailed procedures.

Authorizing Use of Equipment at a Telecommuting Site

Use of any university-owned equipment at a designated telecommuting site must be authorized by way of a properly executed Off-Campus Property Permit submitted to Purchasing and Property Services.

Enabling Remote Computer Access

Employees may be authorized to access their workplace computer if they have appropriate Internet capability at the designated telecommuting site.

UNIVERSITY OF SOUTH FLORIDA

Telecommuting Agreement

Division of Human Resources

Employee Name: ______________________________ GEMS Employee ID #: ____________________

Position Title: ______________________________ College/Div./Dept.: Florida Institute of Oceanography

Classification: □ Faculty □ Administration □ Staff* □ Temporary/OPS*

The Division of Human Resources ("DHR") must approve any telecommuting agreement involving non-exempt, hourly-paid employees prior to implementation.

Duration: This agreement will be valid as specified below until terminated by the employee or management.

Termination of Agreement: The employee may discontinue the telecommuting arrangement at any time. Also, management may discontinue the telecommuting arrangement at any time if it is not in the best interest of the university. Termination of the agreement by either party must be in writing. https://usfweb.usf.edu/human-resources/resources/showfile/2/106

Place of Work: The employee agrees to work at the regular work site and/or the designated telecommuting site and not at an unapproved site. The supervisor may require the employee's presence at and participation in meetings, training sessions, and/or other work-related activities.

Work Hours: Work hours are specified below. Any deviation from the specified work hours must be approved in advance by the supervisor. The employee should not be responsible for care-giving for children, parents, or others during scheduled hours of work.

Basis for Entitlements: All pay, leave, and travel reimbursement entitlements will be based on the employee's regular work site, not the designated telecommuting site. The employee does not forfeit any reimbursement for authorized expenses incurred while conducting business for the university.

Leave: The employee must obtain supervisory approval before using leave, in accordance with established procedures.

Overtime: If the employee is eligible to receive compensation for overtime (i.e., overtime pay and/or compensatory leave), he/she must receive supervisory approval for such overtime in advance of working the time.

University Equipment: In order to effectively perform work, the employee may be authorized to use university equipment at the designated telecommuting site. The equipment must be protected against loss, damage, and unauthorized use. Equipment provided by the university will be maintained and serviced by the university. Access to university equipment at the telecommuting site must be granted to appropriate officials. Equipment provided by the employee will be at no cost to the university and will be maintained and serviced by the employee.

Personal Property Liability: The University will not be liable for damages to the employee's property resulting from the telecommuting arrangement.

Costs: The University will not be responsible for operating, maintenance, or other incidental costs associated with use of the employee's residence as the designated telecommuting site.

Workers' Compensation: The employee is covered by workers' compensation for an injury or illness resulting from performing official duties at the designated telecommuting site. The employee must authorize appropriate officials access to the telecommuting site to perform safety inspections and/or investigate a workers' compensation claim.

Work Assignments: Unless other arrangements are made between the employee and the supervisor, the employee will periodically meet with the supervisor at the regular work site to receive assignments and to review completed work. The employee will complete all assigned work according to procedures and timelines mutually agreed upon with the supervisor.

Supervisor Visits: The supervisor may visit the designated telecommuting site with advanced notice to the employee. The purpose of such visits is to ensure proper maintenance of any equipment provided by the university, confirm that the site is conducive to the telecommuting arrangement, observe work being performed, and/or for other business-related reasons.

Performance Evaluation: The evaluation of the employee's job performance will be based on established performance standards and expectations. Performance must remain at an overall satisfactory level for the telecommuting arrangement to continue.

Official Documents/Records and Other Information/Data: While working at the telecommuting site, the employee will properly safeguard documents/records from loss, damage, or unauthorized access and prevent unauthorized access to any sensitive or confidential information and data via computer or other telecommunications, as applicable.

Participation in Evaluation of Arrangement: When requested, the employee and supervisor will be expected to promptly complete and submit telecommuting evaluation materials.

Failure to Comply: Non-compliance with the provisions and conditions of this agreement may result in termination of the agreement and telecommuting arrangement and/or appropriate disciplinary action.

Telecommuting Begin Date: ________________ End Date: 4/6/2020

Address of Telecommuting Site:

Work Schedule at Telecommuting Site:

Work Schedule at Regular Work Site:

Equipment / Services Provided by Employee:

Equipment / Services Provided by the University:

Other Conditions: Employee must agree to log into TEAMS and open work email at the start of their assigned work schedule and keep the applications open throughout the scheduled shift. Work plan must also be attached to this request.

We understand and agree to the provisions and conditions specified in this agreement. We have discussed and agreed to procedures for permitting any deviations to this agreement.

______________________________ ______________
Employee Signature Date

______________________ ______________________ ______________ ________
Supervisor Name (Print) Signature Position Title Date

For non-exempt, hourly-paid (staff) employees

□ Approved □ Not Approved

______________________________ ______________
Division of Human Resources Manager Date

□ Approved □ Not Approved

______________________________ ______________
Vice President / Provost / Designee Signature Date

______________________________ ______________
Vice President / Provost / Designee Signature Date

Work Plan Instructions: Please provide a description of the work you'll be performing during the Telecommuting Agreement period. Please include what those tasks would be and the expected outcome(s). Please include this with when making your Telecommuting Agreement request. Enter a description in the space below.

USF Property can be taken off-campus for official university business only with approval from the supervisor and accountable officer. During the remote working period, if you wish to take USF property such as monitor, printer and etc. to help you perform your work remotely, an Off-Campus Property Permit is required. Please fill out the request and submit to camngo@usf.edu before taking the property off campus.

USF UNIVERSITY OF SOUTH FLORIDA

USF FORM #6028
OFF-CAMPUS PROPERTY PERMIT

Permits are valid for a maximum of one year and must be renewed annually. Property can be taken off-campus for official university business only. Illegible, incorrect and/or incomplete forms will be returned to the custodian unprocessed for corrections and/or clarification.

CHART FIELD COMBINATION (Use one per form.)

Op Unit	Fund	Dept ID	Product	Initiative	Project

USF Tag #	Description	Serial ID	Return	Ret Loc
			□	
			□	
			□	
			□	

From Date	To Date	Purpose	Property Use Address

USF Custodian Name (Type or Print Legibly)	Employee ID#	USF Office Location

I have read and understand the university procedures and requirements regarding off-campus property use. I acknowledge and accept full responsibility for the above-described equipment. I agree to reimburse the University of South Florida for damage or loss resulting from negligence. I understand that I may be charged a daily rental fee for use other than official university business. I understand that this equipment may need to be returned to the university at any reasonable time for inventory verification.

______________________________ ______________
Custodian Signature Date

CUSTODIAN SUPERVISOR AUTHORIZATION (REQUIRED)

______________________________ ✗______________________________ ______________
Supervisor Name (Print) Supervisor Signature Date

ACCOUNTABLE OFFICER AUTHORIZATION (REQUIRED)

______________________________ ✗______________________________ ______________
Accountable Officer Name (Print) Accountable Officer Signature Date

CONFIRM RETURN OF PROPERTY TO UNIVERSITY

When USF equipment is returned to an on-campus location, indicate above the building/room the equipment was returned to. If it is a partial return, indicate above which items were returned by putting a checkmark in the "Return" column. Confirm your return of this equipment by providing the signature below of the authorized Accountable Officer. Illegible, incorrect and/or incomplete forms will be returned to the custodian unprocessed for corrections and/or clarification.

______________________________ ______________
Accountable Officer Return Verification Signature Date

SEE EXCEL WORKBOOK FOR ACTUAL TEMPLATE

Instructions: Please keep track of the work performed while engaging in remote work . Return this workbook to Cam Ngo at camngo@usf.edu at the conclusion of the approved Telecommuting period.

Employee Name:	Enter first and last name here	Employee ID:	Enter Employee ID here	Classification:	Enter either Faculty, Administration, Staff, OPS

Date	Start Time	Finish Time	Description Task Performed	Meetings Conducted

Working Remotely Tips

PASSWORDS

Some people have websites continuously logged in. Make sure you know your passwords so you can log in remotely.

GEMS and FAST

Make sure that you can log into GEMS or FAST remotely via https://my.usf.edu. You must also be able to do the Two Factor Authentication—**remotely**. If your authentication is through your work phone, you will NOT be able to access GEMS off campus.

Bookmarks

Know how to access your bookmarks from off campus if you need them. You can export them as a file.

- Firefox: https://support.mozilla.org/en-US/kb/export-firefox-bookmarks-to-backup-or-transfer
- Chrome: https://support.google.com/chrome/answer/96816?hl=en

Email and other Office 365 functions

1. Go to https://my.usf.edu
2. Log in with your NetID and password.
3. Under Email, select USF Office 365

Other Microsoft Office apps are also available with the grid icon (on a PC desktop, it's in the upper left corner). There you can access Word, Excel, Teams, and other functions.

Client installation is available here: https://www.usf.edu/it/documentation/office365/personal-download.aspx

Box

To access Box online, go to http://box.usf.edu/. Use your full email address as the login and your NetID password as the password.

NEW VPN access-Palo Alto GlobalProtect

Instructions for accessing, downloading and using the Palo Alto client will continue to be found by visiting https://vpn.usf.edu also see below for instructions.

Other Useful IT links

- IT Documentation: https://www.usf.edu/it/documentation/
- USF Application Gateway: https://www.usf.edu/it/apps/

Docusign

Need to sign a document? USF has a license for Docusign. And the Psychology Department did this handy tip sheet with instructions: https://www.usf.edu/arts-sciences/departments/psychology/documents/docusign.pdf

Remote Desktop Connection

This is handy for accessing your work computer from home. However, your work computer needs to be turned on for this to work. If there was, for example, a quick power outage, your computer will shut down, so please do not rely on this! Make sure you can access what you need from a home computer as well: https://www.usf.edu/it/documentation/remote-desktop-gateway.aspx. You will need to know your computer name or IP address.

Other resources:

- https://www.cdc.gov/coronavirus/2019-ncov/index.html
- https://www.usf.edu/coronavirus/index.aspx

Microsoft Teams Cheat Sheet

Logging in

- Visit teams.microsoft.com in your browser or log-in to USF Microsoft Office 365 (via myUSF) and open the app menu
- OR Download the desktop client for your machine: https://www.usf.edu/it/documentation/office365/microsoft-teams.aspx
  - The browser version of Teams sometimes has more features and greater usability than the desktop app; this is especially true for MAC users

Teams Parts

- **Team**: made up of people in the same department or working group that often work together on projects
- **Channel**: an area to chat within a Team (like Slack); a Team can have multiple channels
- **Planner**: can be made to keep track of tasks in specific projects (a lot like Trello, similar to Asana); a Team can have multiple Planners per team
- **Chat**: an area where you can chat with one or more individuals separate from a Channel (similar to Slack's direct messages)

Notifications

- 'Follow' a channel, by clicking the three dots at the end of the Team title and selecting 'notifications' to set your preferences and get notice when someone posts in that channel
  - If you have not allowed notifications on any channel, the Teams dashboard will show you which of your teams has unseen activity by bolding the titles
- @mention someone if you want to be sure they see your comment/message in a channel

Files

- You can add attachments to a chat and/or a channel
  - When adding attachments to a channel, those files will be listed in the 'Files' tab of the Team
- You can load files and folders directly into the 'Files' tab in a Team
  - Recommended: to control versioning, link a Box file instead of loading files to Teams
  - Share the Box file with your Team: only those team members who have access to Box will be able to access the content you have linked to your team.

Teams Meetings

Team meetings can be created from within a Team or from Outlook (desktop application); creating a meeting in Teams automatically creates a virtual meeting space and connection information (phone and online)

- From within Teams: Click on the Calendar (Calendar) icon on the left and select 'new meeting' OR click on the camera (📹) icon under the chat field in a channel to 'meet now'
  - The camera icon in the top right corner of a 'chat' will also allow for immediate meetings
- From Outlook: open your calendar and select 'New Teams Meeting' from the action ribbon

**You can invite non-Team members to a Team meeting (including participants outside of USF)*

Download and Install the GlobalProtect App for Windows

Before connecting to the GlobalProtect network, you must download and install the GlobalProtect app on your Windows endpoint.

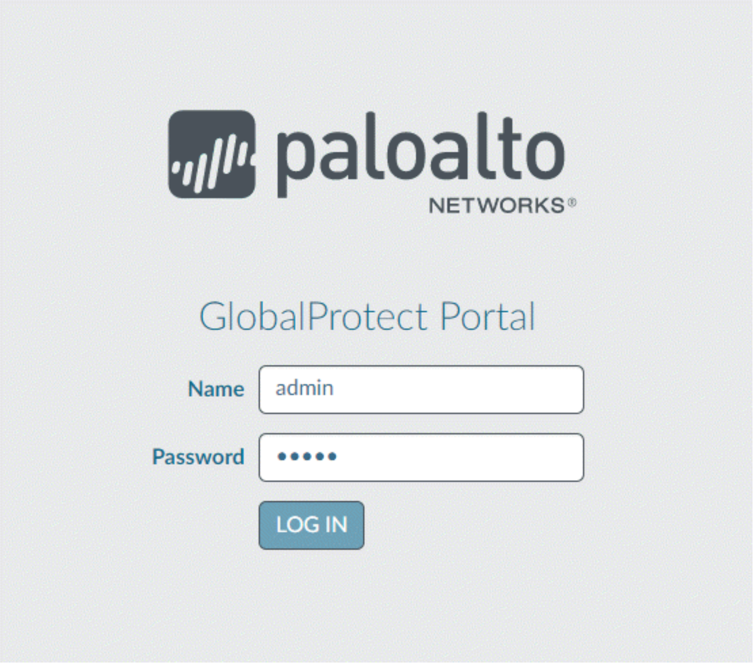
Use the following steps to download and install the app:

To run GlobalProtect app 5.0, Windows endpoints require Visual C++ Redistributables 12.0.3 for Visual Studio 2013. If you have not already installed any redistributable packages on your endpoint, the GlobalProtect app installs Visual C++ Redistributables 12.0.3 automatically. If you have already installed Visual C++ Redistributables 12.0.2 or an earlier release, you must either uninstall the existing redistributable packages from your endpoint or upgrade to Visual C++ Redistributables 12.0.3 prior to installing the GlobalProtect app.

STEP 1 | Log in to the GlobalProtect portal.

1. Launch a web browser and go to the following URL:
   `https://vpn.usf.edu`

2. On the portal login page, enter your **NetID** and **Password**, and then click **LOG IN**.



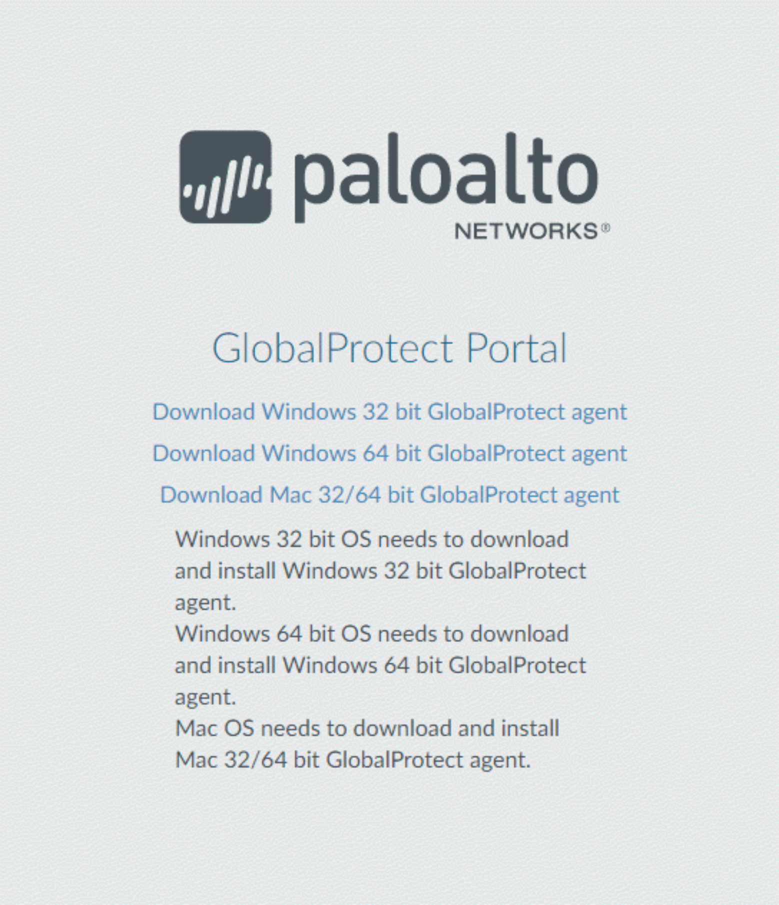
GlobalProtect Portal

Name admin

Password •••••

STEP 2 | Navigate to the app download page.

In most instances, the app download page appears immediately after you log in to the portal. Use this page to download the latest app software package.



paloalto NETWORKS®

GlobalProtect Portal

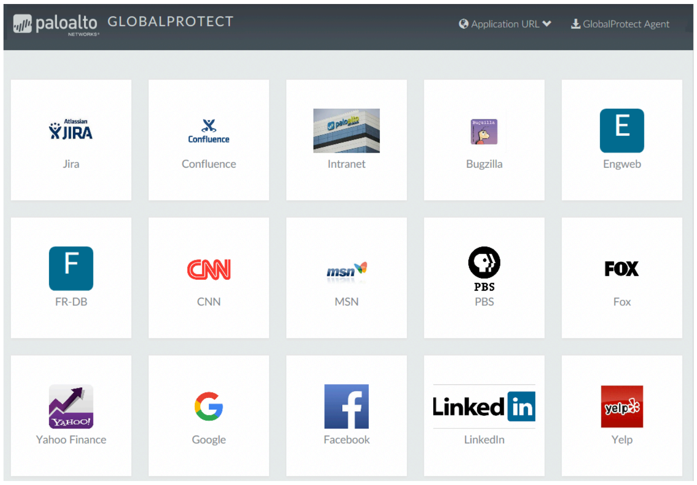
Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

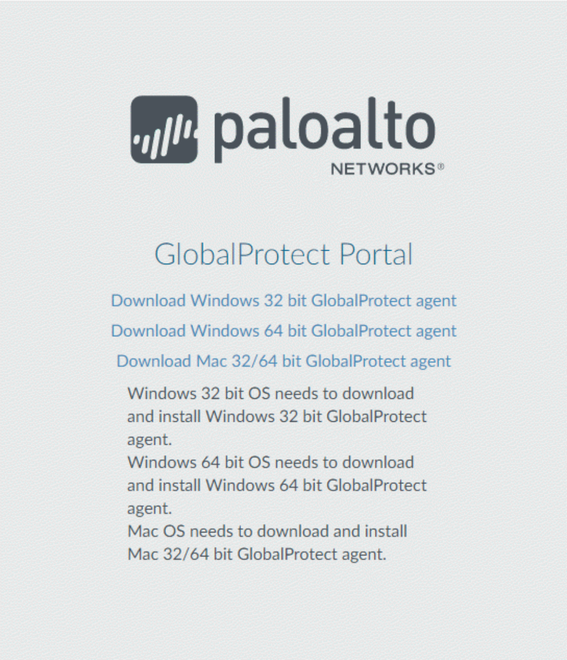
Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

If your system administrator has enabled GlobalProtect Clientless VPN access, the applications page opens after you log in to the portal (instead of the app download page). Select **GlobalProtect Agent** to open the download page.



STEP 3 | Download the app.

1. To begin the download, click the software link that corresponds to the operating system running on your computer. If you are not sure whether the operating system is 32-bit or 64-bit, ask your system administrator before you proceed.



paloalto NETWORKS®

GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

2. Open the software installation file.

3. When prompted, **Run** the software.

4. When prompted again, **Run** the GlobalProtect Setup Wizard.

STEP 4 | Complete the GlobalProtect app setup.

1. In the GlobalProtect Setup Wizard, click **Next**.

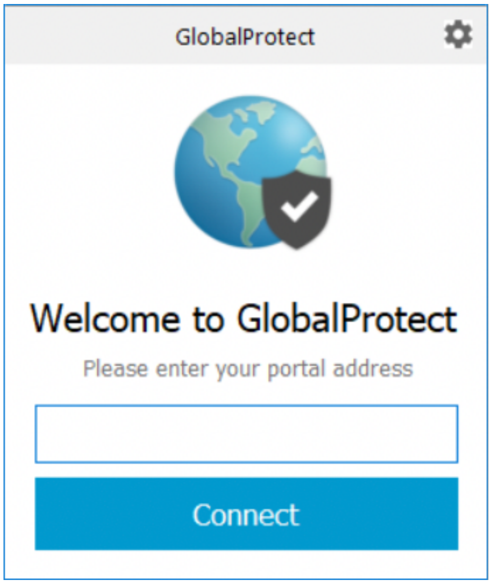
2. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks\GlobalProtect), or click **Browse** to select a new location and then click **Next** twice.

3. After installation is complete, **Close** the wizard.

STEP 5 | Log in to GlobalProtect.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.

2. Enter vpn.usf.edu, and then click **Connect**.



GlobalProtect

Welcome to GlobalProtect

Please enter your portal address

3. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, select the gateway from the **Gateway** drop-down (for external gateways only).
   This option is only available if your administrator enables manual gateway selection.

4. Click **Connect** to initiate the connection.

5. (Optional) If prompted, enter your **Username** and **Password**, and then click **Sign In**. If authentication is successful, you are connected to your corporate network, and the status panel displays the **Connected** or **Connected - Internal** status. If your administrator sets up a GlobalProtect welcome page, it displays after you log in successfully.

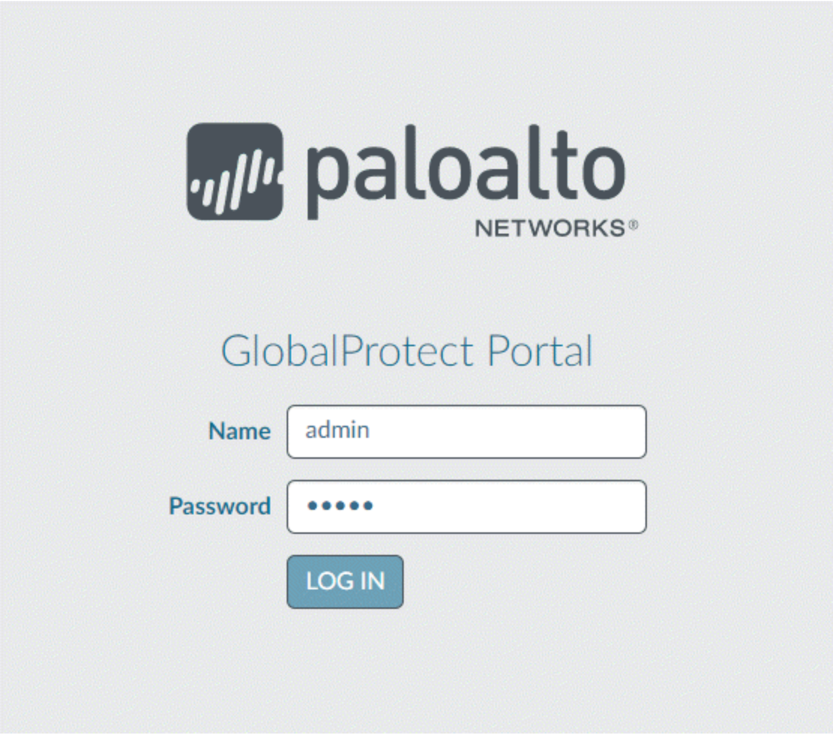
Download and Install the GlobalProtect App for Mac

Before connecting to the GlobalProtect network, you must download and install the GlobalProtect app on your Mac. Use the following steps to download and install the app:

STEP 1 | Log in to the GlobalProtect portal.

1. Launch a web browser and go to the following URL:
   `https://vpn.usf.edu`

2. On the portal login page, enter your **NetID** and **Password**, and then click **LOG IN**.



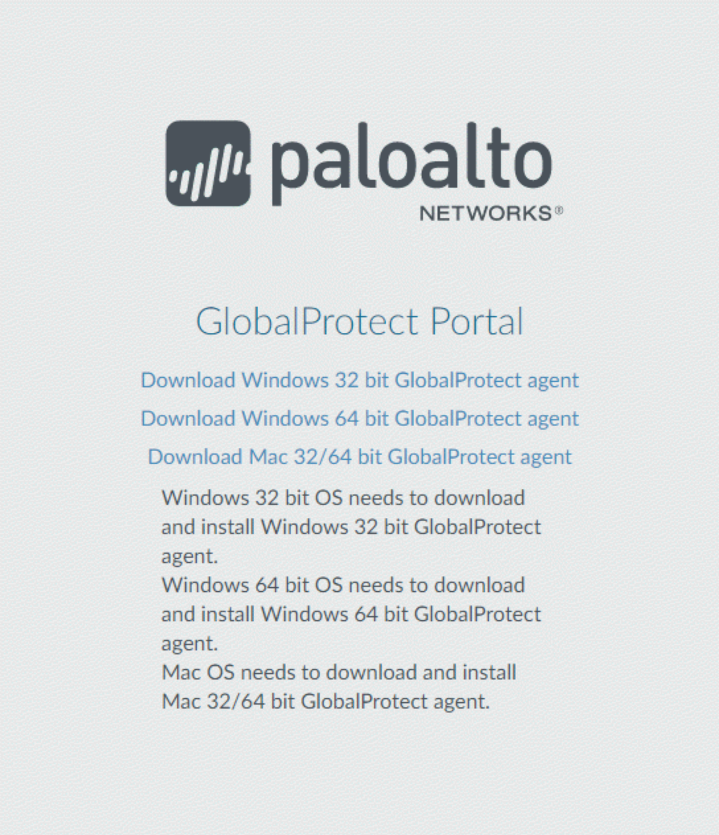
GlobalProtect Portal

Name: admin

Password: •••••

STEP 2 | Navigate to the app download page.

In most instances, the app download pages appears immediately after you log in to the portal. Use this page to download the latest app software package.



GlobalProtect Portal

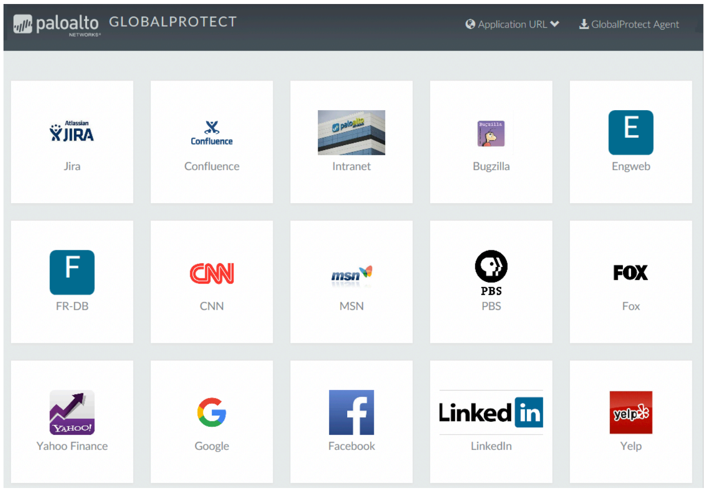
Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

If your system administrator has enabled GlobalProtect Clientless VPN access, the applications page opens after you log in to the portal (instead of the app download page). Select **GlobalProtect Agent** to open the download page.



STEP 3 | Download the app.

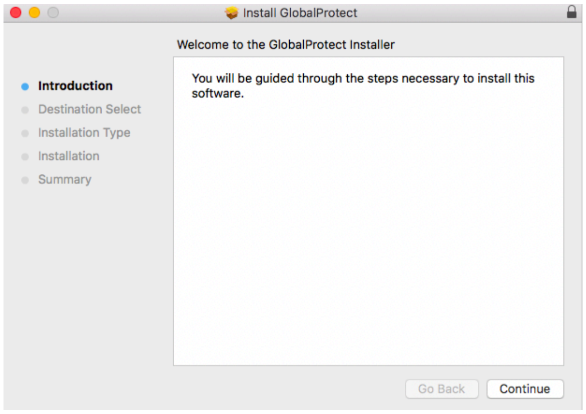
1. Click **Download Mac 32/64 bit GlobalProtect agent**.

2. When prompted, **Run** the software.

3. When prompted again, **Run** the GlobalProtect Installer.

STEP 4 | Complete the GlobalProtect app setup using the GlobalProtect Installer.

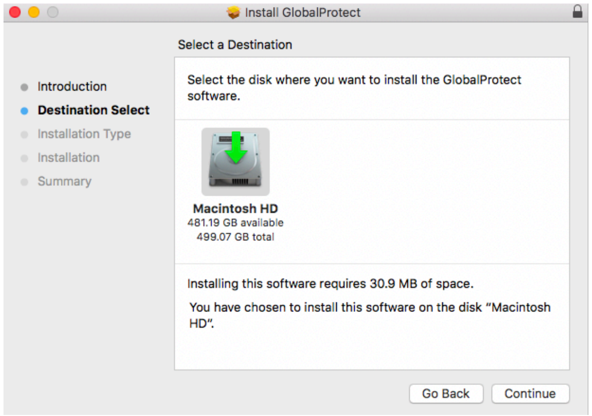
1. From the GlobalProtect Installer, click **Continue**.



Welcome to the GlobalProtect Installer

You will be guided through the steps necessary to install this software.

1. On the **Destination Select** screen, select the installation folder for the GlobalProtect app, and then click **Continue**.



Select a Destination

Select the disk where you want to install the GlobalProtect software.

Macintosh HD
481.19 GB available
499.07 GB total

Installing this software requires 30.9 MB of space.

You have chosen to install this software on the disk "Macintosh HD".

2. On the **Installation Type** screen, select the **GlobalProtect** installation package check box, and then click **Continue**.

3. Click **Install** to confirm that you want to install GlobalProtect.

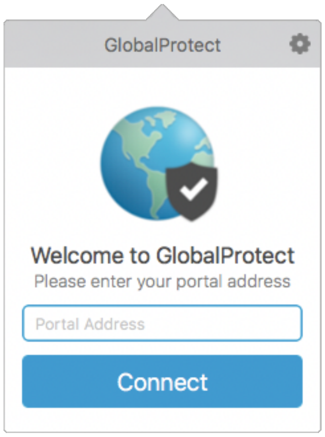
4. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to begin the installation.

5. After installation is complete, **Close** the installer.

STEP 5 | Log in to GlobalProtect.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.

2. Enter vpn.usf.edu, and then click **Connect**.



3. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, select the gateway from the **Gateway** drop-down (for external gateways only). *This option is only available if your administrator enables manual gateway selection.*

4. Click **Connect** to initiate the connection.

5. (Optional) If prompted, enter your **Username** and **Password**, and then click **Sign In**. If authentication
   is successful, you are connected to your corporate network, and the status panel displays the **Connected** or **Connected - Internal** status. If your administrator sets up a GlobalProtect welcome page, it displays after you log in successfully.