



# **SDF VPN**

## **Work Instruction & Guidance**

February 2022  
Revision 4

# Global Proving Grounds & Test Laboratories

## SDF VPN Configuration and User Guide

---

### SDF VPN Access Request Process

### First Time Setup Process

### Connecting to SDF VPN: Day-to-Day usage

### Frequently Asked Questions

**This work instruction will provide the necessary steps to ensure connectivity to devices in the SDF environment.**

- Lab devices are migrating into an isolated network to protect GM from security risks. (Software Defined Fence)
- To remotely connect to lab devices from your assigned asset, you must connect using a VPN profile customized for the lab environment.

### **Audience**

GM employees that require Remote Access for viewing, configuring, and supporting lab devices behind the SDF Firewall.

### **Out-of-Scope**

Vendor, Non-GM badged employees and 3<sup>rd</sup> party Remote Access

# SDF VPN Access Request Process

# Submit Galileo Request

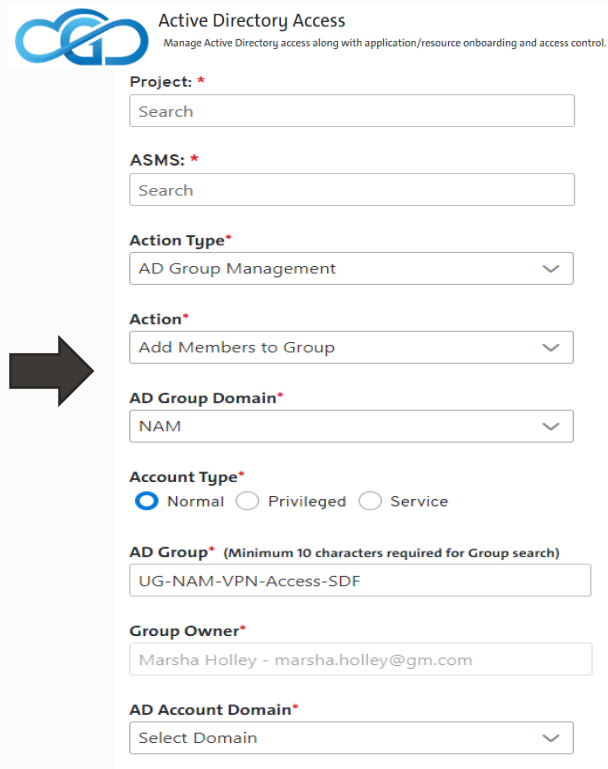


1. Open web browser to: <https://galileo.gm.com>
2. Click Services, Access Management, IAM-Active Directory Access, Get Started

## [Active Directory Access \(gm.com\)](#)

### 3. Request form guidance

Project	Choose a project that relates to why you need SDF access. Enter a couple of random letters in the field and press enter; you will get a drop down list of projects you can choose from. Note: Some bucket type projects can be added as well.
ASMS / Application	<p>Type &lt;ASMS name OR ASMS number&gt; search results. The owners this ASMS will need to approve your request.</p> <p>Your ASMS number should relate to the application(s) you work with. If you navigate to sites.gm.com and enter your application in the search field you should get a list of relevant ASMS numbers. You can click on each one individually for a more complete description. If you just cannot decide on one that relates to your daily work you can use 185713 for the ASMS number in this request.</p> <ul style="list-style-type: none"><li>• It is strongly recommended to become compliant with an approved ASMS ID.</li></ul>
Action Type	AD Group Management
Action	Add Members to Group
AD Group Domain	NAM
AD Group	UG-NAM-VPN-Access-SDF
Group Owner	Marsha Holley (should auto-populate) You may be contacted to validate your request
AD Account Domain	NAM
Account Type	Normal
Add Accounts	<add the ID's being requested>



**Active Directory Access**  
Manage Active Directory access along with application/resource onboarding and access control.

**Project:** \*

  
**ASMS:** \*  
**Action Type:** \*

AD Group Management

**Action:** \*

Add Members to Group

**AD Group Domain:** \*

NAM

**Account Type:** \*

☒ Normal ☐ Privileged ☐ Service

**AD Group:** \* (Minimum 10 characters required for Group search)

  
**Group Owner:** \*  
**AD Account Domain:** \*

Select Domain

# First Time Setup Process

# Cisco AnyConnect VPN Client Configuration



## Prerequisite:

**Your GMID MUST be provisioned to the SDF VPN Active Directory User Group first!**

### GM-Online or EDWS device

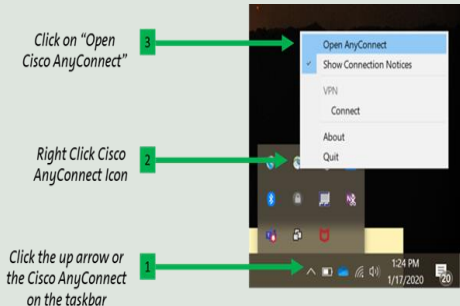
- Must have a valid GM VPN Certificate template
- Must have updated antivirus definitions
- Must have Cisco AnyConnect VPN Client v4.60456 +

### GMID

- Must be in the SDF VPN Active Directory user group
- Must be logged in using your GMID that was added to the SDF VPN AD security group

## STEP 1

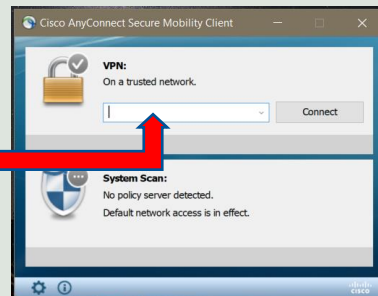
Open Cisco AnyConnect from your taskbar by right clicking on the AnyConnect icon.



## STEP 2

### Download the SDF VPN Configuration Profile

In the drop-down text box, type the URL (below) based on your **current network location:**



**You are NOT in a GM building connected to the GM Network:**  
**Naeraha18.ext.gm.com or naeraha17.ext.gm.com**

**You ARE in a GM building and connected to the GM network:**  
**dcmnsciv019-vi2892.edc.nam.gm.com**

If for some reason this is not working when onsite, you can connect your computer to a hotspot on your phone which will get you internet access

## STEP 3

### Click connect

- Your PC will now connect to the SDF VPN and download the required network certificates to your device.
- When complete, you should get a notification and be disconnected. If not, you can manually disconnect.
- You will now have 4 new SDF VPN profiles added to the global dropdown list: EXT/INT Milford & Warren.

# Connecting to SDF VPN

## Day-to-Day usage

# SDF VPN Overview



Use the Cisco AnyConnect VPN client to connect & access to lab PCs and devices for viewing, configuring, and supporting lab devices within the Global Test Lab environment.

## Requirements

### GM-Online or EDWS device

- Must have a valid GM VPN Certificate template
- Must have updated antivirus definitions
- Must have Cisco AnyConnect VPN Client v4.60456 +

### GMID

- Must be in the SDF VPN Active Directory user group
- Must be logged in with your GMID that has SDF VPN access

## Cisco AnyConnect SDF VPN Connection Options

### Externally / offsite *(home, coffee shop, mobile hotspot, non-GM location)*

- **EXT SDF Milford**
- **EXT SDF Warren**

### Internally / onsite *(while at GM and connected to GM network)*

- **INT SDF Milford**
- **INT SDF Warren**

*This only provides the connection to the Lab SDF Environment.  
Local Remote Access tools and applications are still required.*

## SDF VPN Connection and Usage Notes

- You must manually connect to GM and SDF networks
- When external / offsite, VPN might not automatically connect to GM

## Allowed / Disallowed Functionality and Limitations

Allowed Functionality	Disallowed Functionality
Connect to lab devices the same way as you did on the GM network (e.g. VNC, RDP, Share Drive Mapping, etc...)	Using a lab device as a jump server to connect to EDC resources restricted by the VPN
<ul style="list-style-type: none"><li>• Collaboration Services: Teams, O365 (Office, email, teams), webmail</li><li>• <a href="#">Limited external internet access</a></li></ul>	<ul style="list-style-type: none"><li>• GM EDC hosted Applications, thick-client apps</li><li>• Email client, (unless provisioned in O365)</li></ul>
Access to EDC DFS shares specific to TCWS	EDC Isilon/SAN storage not associated with TCWS

- *Follow the SDF VPN user onboarding instructions*
  - *GM-Online devices should meet these requirements.*
- If you have issues, please contact IT Site Services for Support.*

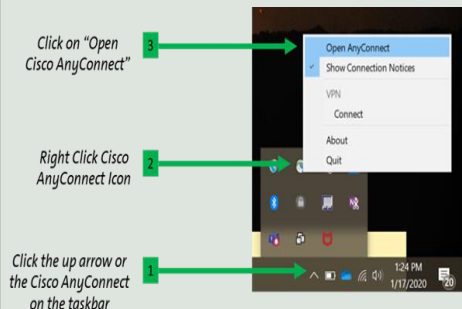


# Cisco AnyConnect VPN Client Connection



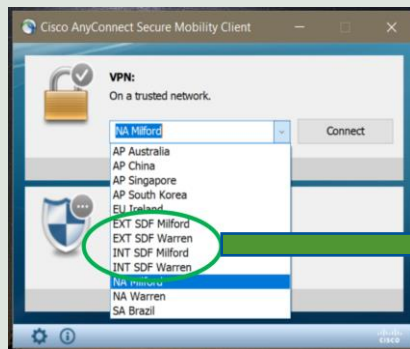
## STEP 1

Open Cisco AnyConnect from your taskbar by right clicking on the AnyConnect icon.



## STEP 2

Choose an Internal or External SDF VPN Profile that is nearest to your location:



### Cisco AnyConnect SDF VPN Connection Options

Externally / offsite (home, coffee shop, mobile hotspot, non-GM location)

- **EXT SDF Milford (Preferred)**
- **EXT SDF Warren**

Internally / onsite (while at GM and connected to GM network)

- **INT SDF Milford (Preferred)**
- **INT SDF Warren**

## STEP 3

Click connect

- Your PC will now connect to the SDF VPN

### Reminder

- You must manually connect between GM Employee and SDF Lab networks
- When external / offsite, the VPN client may not automatically connect to GM Employee VPN

# Limited external internet access



Connecting to GM data center internal web applications may require Multi-Factor Security



Connect to SDF VPN

Open Internet Browser

Multi-Factor Authentication  
User Validation

User Verification

External websites / URLs may have restrictions in place.  
External sites must be approved for business purposes.


Your User ID must have Multi-Factor Authentication  
enabled and configured

# Frequently Asked Questions

# Frequently Asked Questions



- **I cannot submit an access request into Galileo.**
  - At this time, Galileo requests must be submitted by GMIT. Please work with your IT support staff, IT innovation, or IT liaison to submit your request.
- **Will I be able to copy files to and from my GM-Online or EDWS computer while in the SDF network?**
  - Yes, file transfers are allowed while connected to the SDF VPN, but are limited to TCWS DFS shares only.
- **Can I access the internet after I connect to the lab VPN?**
  - Yes. Limited access is allowed for collaboration services, ie. Office 365, teams, and email.
  - I need to access some EDC hosted applications and data from my computer after I connect to the SDF VPN, is that possible?
  - Yes/No. Most internal applications will be restricted while connected to the VPN, although you will be able to connect to TCWS data storage resources when connected. To access blocked EDC applications, you are encouraged disconnect from the SDF VPN and reconnect to Employee VPN. (if in the office, your pc will auto-connect to the GM network)
- **I need to collaborate with other engineers to configure tests. Can I use Teams to message, attend meetings, and share my screen?**
  - Yes. Teams is allowed when connected to the SDF VPN.

- **Can I access my email, teams or other non-lab GM applications?**
  - Yes/No. If your email services have migrated to Office 365 cloud services, then email will not be impacted. Otherwise to access these resources, you are encouraged disconnect from the SDF VPN and reconnect to Employee VPN. (if in the office, your pc will auto-connect to the GM network)
  - If you don't have O365 email, please use GM's web-based email:  
<http://outlook.com/owa/generalmotors.onmicrosoft.com>  
formally: <http://webmail.gm.com>
-  ➢ SDF VPN is to used to support and manage lab devices only. If there are EDC specific applications that are critical to manage or configure lab devices, firewall rules can be added with support from the application owner.
- **I cannot install the required SDF Lab VPN Certificate on my client when remote. I get an error message that says the server cannot be found or resolved, contact your system administrator.**
  - Some GM-Online systems may encounter this issue due to cached network configurations. Try the following steps to resolve:
    - a) Your GMID must be provisioned to use the SDF VPN (see onboarding steps)
    - b) Ensure you have an active internet connection and you can connect to Employee VPN.
    - c) Try both external url's listed in the documentation
    - d) If the documented url's do not work, try the following url: [dcminsciv019.ext.gm.com](http://dcminsciv019.ext.gm.com)
    - e) If that does not work, try installing the certificate from a local GM network on-site.