celestix

InstaSafe Solution for Corporate Domain Joining

Join remote computers to corporate domain through InstaSafe Secure Access Solution

Why is Domain Joining So Important?

Large enterprises with a distributed workforce that are working in remote offices, branch offices or even from home offices provide their employees with laptops in many different ways. They ask the employee to buy a recommended laptop locally and reimburse them and then get the user to install all the required corporate applications and security software; or they ship preconfigured laptops over to them. Shipping across laptops to employees is mostly cumbersome and challenging for many reasons.

However, while the benefits of having employees buy laptops locally are many, the IT team face numerous challenges to get the endpoints to comply with corporate policies; far less have the laptop join the corporate domain through which it would be very easy for the IT team to manage the laptop like they do to the systems located in their office.

Enterprises have been unable to have remote computers join the corporate domain as it is not possible to expose the Domain Controller (DC) to the internet without exposing the entire network to a huge security risk. As such, all remote user computers are running in isolation leaving risk and compliance teams in a catch 22 situation.

Need for Domain Joining

IT teams want to have the remote computers join the corporate domain so that they can easily push group policies, have the remote computers pull updates, patches and therefore comply with corporate security policies. However, as domain joining activity requires many protocols and ports access to be provided to the computer and the DC cannot be exposed to the internet with all the required ports open as it poses huge risks.

Our Solution

- InstaSafe Secure Access allows you to keep your DC in the private network and secured with the firewall blocking all inbound ports.
- The access to the DC is provided by the InstaSafe Gateway, located in the same network as the DC.
- The InstaSafe Gateway creates a tunnel from the internal network to the InstaSafe Controller.
- The Controller is the central enforcement point to interconnect the Users to the applications (including the DC) in the data center.
- The client computer has the InstaSafe Client running as a service.
- This ensures that the InstaSafe Client always starts immediately when the computer is started.
- As the InstaSafe Client starts, it detects an internet connection and establishes a connection to the InstaSafe Controller.
- The InstaSafe Client then provides the user certificate and the device fingerprint to the InstaSafe Controller.
- The InstaSafe Controller authenticates the user computer transparently using the certificate and the device fingerprint to ensure that only authorized users and their computers can connect.
- Once authenticated, the User is provided access to the DC through the InstaSafe Gateway tunnel.
- Now, the user can go through the normal steps to join the computer to the corporate domain.

celestix

Celestix Networks, Inc.
4125 Hopyard Road #225
Pleasanton, CA 94582
www.celestix.com

Americas : +1 510.668.0700
EMEA : +44 (0203) 900 3737
Asia : +65 6958 0822
sales@celestix.com