Link to article: https://discover.claromentis.com/knowledgebase/articles/798

How we connect to On-Premise servers - Splashtop

Please note: This only applies if you are hosting Claromentis within your own infrastructure

This article is in reference to the following News article that was published 4th June 2020 -here.

Introduction

To help assist you with the support requests, installations, and ongoing maintenance that form your support contract, we need remote access to the web and/or database server that hosts your Claromentis intranet. We want to let you know that we're making some changes to the way we access your servers so that we can deliver the best possible levels of support to you and your staff.

From 8th June 2020, we're removing support for various methods of remote access and streamlining access to one product called Splashtop.

We've been researching and testing the implementation of a single remote connection method that will work for all of our on-premise customers, and we believe that Splashtop will allow us to support you effectively, securely, and quickly.

What changes we're making

From the 8th of June 2020, we will no longer be supporting the following methods of remote connection:

- Screen share
- Outdated access gateways/VPN servers
- Any remote access method that doesn't support macOS and Windows.

We will instead be asking you to install the Splashtop agent - Please see instructions on how to install thishere.

Why we're removing support for multiple remote access methods

We've always tried to be as flexible as possible to facilitate the various methods for connecting to remote servers. However, as our customer base has grown and our policies and procedures have matured in line with security best practices, this flexibility has led to a few challenges.

- **Screen share:** In some cases, server access has been limited to screen share only. Whilst we appreciate that customers have been very flexible with timings, restricting access to screen share makes it difficult for us to arrange connections at specific times, especially across different time zones. The nature of screen shares also means the keyboard or mouse control becomes unresponsive, making it difficult to troubleshoot and fix issues quickly. With such a range of screen share tools available on the market, it also adds another threat vector.
- **Outdated access gateways/VPN servers:** As part of our policies to prevent security vulnerabilities, we always update to the latest versions of access gateway plugins or VPN clients. This means we cannot access certain customer systems if they are running older versions of the server.
- **Support for Claromentis endpoints:** The majority of our team are based on macOS and to connect with a Windows Virtual Machine would be a breach of our internal security policies.

- **Shared accounts:** Remote access that is limited to one shared account is unfortunately against our security policy. We require that all of our support team members have unique accounts on a least-privilege basis.

Why we're switching to Splashtop

Streamlining remote access to one solution means we can connect to your servers quickly and securely, providing you with faster response times and fixes. Here's why we chose Splashtop:

- Splashtop works in the same way as screen share software, but securely over HTTPS., Therefore, it doesn't require labour-intensive tasks such as firewall changes, account provisioning/maintenance, nor does it require support for VPN/Access Gateway/RDP.
- Every support team member has their own unique account, which is monitored and audited. We can even record each session to comply with highly regulated industry practices.
- Splashtop is SOC 2, ISO 27001, GDPR, PCI and HIPAA compliant: https://www.splashtop.com/compliance.
- Splashtop is secure - here is a breakdown of the Splashtop security features: https://www.splashtop.com/security-features.
- It allows unattended remote access, by simply installing the secure Splashtop agent on the server you'd like our team to access.
- Although unattended remote access is our preferred method, it's possible to configure the Splashtop agent so that it only allows access once approved by your team.
- Splashtop supports Windows, macOS and Linux.
- We ensure that only the team members who require access are granted permission to do so, and we have an acceptable use policy that guides them on credential management, secure passwords, and multi-factor authentication.

Licensing / costs

We don't want you to have to worry about licensing costs for our remote access, and so we're covering the costs of Splashtop as part of your existing support contract - there will be no additional costs to you.

And finally…

We aim to constantly improve the service we offer and believe Splashtop will allow our team to provide a better level of support for you and your team. If you have any questions about this or would like to know more, please take a look at our installation guide or submit a support ticket and we'd be happy to help.

Created on 9 April 2021 by Mike Leggatt. Last modified on 22 April 2021
Tags: access, on premise, Splashtop