Continent-RA
Version 4
Release notes for build 4.1.689.0

This document contains a description of features, operational aspects and limitations of Continent-RA, Version 4, build 4.1.689.0, which must be considered during its operation.

Table of contents

1. Modifications and new features

1. Plugin architecture in which cryptographic algorithms are implemented in the standalone CSP.
2. Registration of events fully described in text form in Windows application log and log files.
3. Capability to gather diagnostic information.
4. Registration of a workstation.
5. User interface with custom color schemes.
6. Automatic download of CRL.
7. Automatic detection of CDP from certificates to update CRL.
8. Connections using two types of protocols – version 3.X (to the Access Server) and 4.X (to the Security Gateway).
9. Automatic connection to the Access Server/the Security Gateway after starting the system using a default profile.
10. Profiles to connect to the Security Gateway (the 4.X protocol).
11. Import of profiles created with the 4.X protocol.
12. Automatic reconnection if the connection is dropped (5 attempts).
13. Two types of authentication using the 4.X protocol (certificate-based or using a login and a password).
14. Automatic detection of system proxy parameters.
15. Easier software installation in one window with minimum user involvement.
16. Quick start of Continent-RA. Capability to import the configuration file and automatic connection.
17. Connections to the Access Server/the Security Gateway can be established before a user logs on to the system. Requires configuring a global profile.
18. Export of the configuration parameters.
19. Two configuration modes of Continent-RA – automatic (import of a configuration file containing all required parameters) and manual.

2. Hardware and software requirements

1	Key carrier	• USB drive; • security tokens and smart cards: Rutoken S, Rutoken Lite, Rutoken Electronic Signature 2.0, Rutoken Electronic Signature 2.0 flash, JaCarta PKI, JaCarta PKI/GOST, JaCarta GOST; • security tokens DS1995, DS1996
2	Operating system	• Windows Server 2016 x64; • Windows Server 2012 R2 x64; • Windows Server 2012 x64; • Windows 10 x86/x64; • Windows 8.1 x86/x64
3	CSP	• Security Code CSP 4.0.xxx • CryptoPro CSP

3. Features and limitations

1. To import a certificate correctly binding it to a key container, the user that imports the certificate must be granted permissions to write and/or modify the following registry subkeys:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Keys
   HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MY\Keys.

2. If the "Root certificate not found" message appears when connecting to the Access Server 3.7, check the following:
   - If a root certificate for a user certificate is installed on the computer with Continent-RA.
   - If a root certificate for a server certificate is installed on the computer with Continent-RA.
   - If the user certificate exists in the database of the Access Server you are connecting to.

3. If an error occurs while connecting with an unconfigured profile created in Continent-RA version 3.7.7, take the following steps:
   - Go to C:\Users\admin\AppData\Roaming\ContinentVPNClient.
   - Open UserConfig.json in any text editor (for example, WordPad).
   - Find the settings of the required connection.
   - For "useCertificate", change the value from "false" to "true".

4. If you install Continent-RA on a computer with Avast Free, you must enable Safe mode of the antivirus and add Continent-RA to the exclusions each time the install blocked warning appears during the installation process or disable the antivirus.

5. To change the settings of CRL and Continent-RA connection profile, you need to run the program as administrator. The only exception is Win 2016 srv, because the user in administrator role can modify settings by default.

6. If CryptoPro CSP and RA 3.7.7.651 are already installed, the system updated to Continent-RA 4 does not support connections with a certificate issued by Security Code CSP. However, connections are supported with a certificate issued by CryptoPro CSP. To fix the problem, delete CryptoPro CSP, restart the computer and run the file with the *.msi extension from the installation disk to install Security Code CSP.

7. If the system connected to the Access Server during the update and does not run after the computer restarts and the "The service not installed" message appears, you need to repair the software from the file with the *.msi extension or through the Microsoft repair tool.

8. If a limited user installs Continent-RA, the program and the entropy gathering process do not run automatically after the system restarts. To continue working, double-click the program shortcut on the desktop or run it from the Start menu.

9. If an administrator installs Continent-RA, the program runs automatically after the system restarts and the target for gathering entropy appears.

10. To redirect all connections via VPN, the respective IPS protections must be enabled on the Access Server. To redirect all the traffic from the computer with Continent-RA through the Access Server when connection is established, the system should not have the route with a metric less than 276. If there is such a route, you must increase the value of the metric or delete the route.

11. Continent-RA 4 is not compatible with Agent of IPS protections, versions 3.7 and 3.9.

12. To use private Rutoken and JaCarta key carriers, you must download and install their drivers.

13. Only certificates issued by CryptoPro CSP can be imported to CryptoPro CSP. You can import certificates issued by either Security Code CSP or CryptoPro CSP to Security Code CSP (certificates compatible with GOST R 34.10-2001).

14. After the CSP is updated, restart the computer.

15. The system cannot contain cryptographic containers with the same name.

16. To use certificates issued in the Access Server remote control on CryptoPro CSP, you must disable checking certificates via CRL. Otherwise, you cannot connect to the Access Server.

17. DNS server address changes are applied only after you restart the program.

18. If the proxy auto-configuration is enabled, to apply changes in the proxy server parameters, restart the program.

19. If you use Continent-RA and Secret Net Studio (SNS) at the same time, we do not recommend denying access to public\continentvpnclient when configuring Mandatory Access Control (MAC). Otherwise, Continent-RA cannot operate.

20. Continent-RA cannot be used as a gateway passing all traffic.

21. Continent-RA supports only keys created using the following parameters: 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. To check the validity of a certificate, go to the certificate properties dialog, click the "Details" tab and select "Public key parameters". Make sure the eighth and the ninth bytes on the left have a value of "02". If the value is different, create a request for a new certificate or import a certificate from an external source.

22. On a computer with English versions of an OS and Continent-RA, a user still can receive notifications and messages from the Access Server version 3.7 and 3.9 in the Russian language. These messages are not going to be translated into English. To view them in Russian, in the OS settings, add Russian for the Unicode programs.

23. If while creating a certificate request, the Access Server 4.X request type was selected, in the "Address" text box, specify the same value specified in the "CommonName" field of the server certificate (the name must be typed in Latin characters without spaces). If the IP address of an Access Server must be specified in the "Address" field, then this IP address must be specified in the "CommonName" field of the server certificate as well. Otherwise, the connection will not be established and the "The address of the access server does not match the name for which the server certificate was issued" message will appear. To fix it, check if all fields are filled in correctly. If the "CommonName" field contains Cyrillic characters or/and spaces, reissue the certificate with correct parameter values.

24. After update, proxy configurations are not imported from Continent-RA version 3.7 to version 4.1 automatically. You need to save the configurations in advance.

25. Pre-logon connection features. Continent-RA makes it possible to connect to the Access Server before user logon, using the global profile. To enable this feature in the settings menu, select "General", then select the "Startup mode" subsection, and select the "Allow Continent-RA to connect before logon" check box (this option is disable by default). To ensure that the feature is enabled, log out. At the top-right corner, the dual monitor icon appears. To connect, click "Logon" and, after the connection is established, log on as user.

26. If the "Allow Continent-RA to connect before logon" is enabled, user logon is slower than usual.

27. Automatic connection using a default profile cannot be established if a user stopped working without disconnecting. In this case, attempting to connect, a user receives a respective message. Terminate the previous connection and run Continent-RA again.

28. The certificate private key is valid for 15 months starting from the beginning of the certificate validity period. When the 15-month period is over, the certificate cannot be used. Reissue the certificate.

29. If the "Request adding other server and root certificates" check box is enabled in general settings:

- connecting to the Access Server using the 3.X protocol for the first time, both certificates (root and server) are added after the request appears on the screen;
- before connecting to the Access Server using the 4.X protocol, the root certificate must be imported. Otherwise, a user receives an error message about the absent certificate. If the root certificate is imported, the server certificate is added automatically after the request appears.

30. If you install Continent-RA on a computer with the English version of SNS 8.4 or 8.5, the Security Code CSP modifies the registry subkey HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\Secret Net Studio\ProductLocale (by changing it to "ru-RU") which may result in an error. To fix it:

- change "ru-RU" to "en-EN";
- install additional libraries to fix this error. To get the required libraries and instructions, contact our technical support.

31. Install third-party CSPs in the same language that is used for Continent-RA.

32. To connect to the Access Server while operating in tandem with CryptoPro CSP 5, you need to enable password saving feature (for example, during the key container test procedure) for the key container that is used for connection using CryptoPro CSP tools.

Trusted Access Technologies

Mailing address:	Silicon Oasis HQ, Wing B, office # A-611, Dubai. UAE | P.O Box
Phone:	+971 43 734 695
	+971 43 591 001
Email:	sales@trustedaccesstech.com
Web:	https://www.trustedaccesstech.com