==========
*** Basic Information ***
==========
[Create date] 2017/06/16

[Program Name] CAP-ES V2 for RE

[Version] 2.4.100.0

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Others

Exported to(language) EUR(en)
[Firmware No.] D592-0001N
[File Information]
 File Name D592-0001N.exe
 File Type Module for Service
 Size 884.62 MB (927596173 byte)
 Check Sum -8Bit Sum: 168B
  -16Bit Sum(Little Endian): 07E5
  -16Bit Sum(Big Endian): 99A6

[Production reflection]

==========
*** Note ***
==========
[Note]

==========
*** Important Notes ***
==========
[Important Notes]

==========
*** Modification History ***
==========
[Modifications made:]
Fixed:
- The user associated billing code information may be deleted by
  task synchronization.
- User associated billing code information (.csv file) that has
  empty domain names cannot be imported.

[Modification history]

Version 2.4.000.0
Support:
- Windows Server 2016 is supported.
- SQL Server 2016 is supported.
- Windows Server 2003/2003 R2/Windows 8 are excluded as support
  environments.

Fixed:
- Update installation from v2.3 to v2.3.100 may fail.
- Offline deactivation may fail.
- When adding a group to the Group Authorization Information List
  via the Administrative Tool, [Color Copy Mode Limitation] may not
  be displayed correctly.
- The error message may not be displayed correctly when
  adding/editing a card ID with many characters.
- Duplicated or deleted cards and errors related to them may not be
  displayed correctly.

Other:
- Billing codes can be obtained from a user attribute.
- Activation method has been changed from server license to client
  access license (CAL).
- A fix for the Apache Commons FileUpload (ACF) vulnerability has
  been added.

Version V2.3.100.0
Support:
1. Support for TLS1.2 has been added.
 *The Java VM version on the device must support TLS1.2.
2. Support for SHA-2 has been added.
 *The Java VM version on the device must support SHA-2.

Fixed:
1. When editing a card ID from lowercase characters to capital
   characters, the edited ID will be deleted after saving the data.
2. Administrator privileges are assigned to users irregularly after
   task synchronization is performed.
3. When trying to newly add an external user who belongs to an

external group to an internal group via a CSV file import, the user will be deleted from the external group.
4. An authentication error will occur and no error will be recorded in CAP-ES when Task synchronization, CSV import, and Delete All Users are executed at the same time and a user tries to authenticate.

Other:
1. RSInfo has been updated.
2. A fix for the Apache Commons Collection (ACC) vulnerability has been added.

Version V2.3.000.0
Supported:
1. Support for Fire Fox ESR 38 has been added.

Fix:
1. In SSL environment, CAP-ES may not be synchronized to external authentication server.
2. If synchronization to external authentication server is performed without proxy user, Jetty may be down and the synchronization fails.
3. When LDAP authentication is performed, E00001 or E03002 error may occur.

Other:
1. Billing Code can be registered to CAP-ES.
2. CAP-ES database can be synchronized between primary and secondary server.
3. Activation site has been changed from GMP server to eDC-i server.
4. RSInfo has been updated.
5. Java version has been updated to 8.

Version 2.2.7.0
Fixed:
1. The built-in user (admin/service) can be registered as a normal user.
2. If a login user name is searched for by using capital letters, the user will not be found in the case that "Convert to Lower Case" is specified in the Login User Name settings under Registration Method in Default Settings.
3. If authentication or synchronization is performed after modifying capital/lowercase letters in the registered user's domain name, 2 users will be registered that only differ by their domain names having capital or lowercase letters. This will cause an authentication error to occur.
4. An internal user's Identification Name can be changed by modifying and importing a Group Authorization Information .csv file.
5. After a user who belongs to an external group is registered in CAP-ES and overwrite importing is performed using an Integrated Information .csv file that does not contain the user, no name

group will be registered to the user.
6. When importing an Integrated Information .csv file, the information log will be incomplete.
7. The message "Enterprise Server Module for CAP V1 Users is to be installed later" will be displayed when confirming whether "Enterprise Server Module for CAP V1 Users" is installed when installing CAP-ES v2.
8. Even if a group is deleted from CAP-ES, the Group Authorization Information List for the group will not be deleted.
9. If an Integrated Information group name is 64 characters or more, the .csv file cannot be imported.
10. The CPU usage for the CAP-ES service may become 100% because of Apache Commons File Upload library instability.
(http://mail-archives.us.apache.org/mod_mbox/www-announce/201402.mbox/%3C52F373FC.9030907@apache.org%3E).
11. If the Account Lock Threshold value set in Active Directory is the same (or less) than the domain controller number specified in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an account lock will occur if the input user's password is incorrect.
12. There is a possibility that SSL 3.0 with a CBC cipher may be decrypted by using a padding-oracle attack.
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566)
13. If multiple domains are specified for "Domain Name" in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an authentication error may occur.

Other:
1. CAP-ES outputs the following logs into the Windows Application Event log:
   - The results of operating a .bat file.
   - When an error occurs.
2. Delete all user information in the CAP-ES database at one time by using "UserAllDelete.bat".
3. The Card ID can be searched for via the User Display Name.
4. A message for confirming if the database is on an internal or external server will be displayed when upgrading. In the case that the database is internal, the database will be updated automatically during the CAP-ES version-up flow. In the case that the database is external, perform the "Create Database" procedure on the external server separately.
5. An attribute on an external authentication server that has multiple values can be specified in "Attribute Name Settings" for card IDs. Up to 10 values (card IDs) are supported.
6. Failover Clustering for Windows Server 2012/2012 R2 is supported.
7. The AES 128/256-bit encryption method can be used for Kerberos Authentication.
8. "SQL Server Name", "Database Instance Name", and "Database Name" can be changed via the Database Management Tool.

==========
*** Basic Information ***
==========
[Create date] 2017/06/16

[Program Name] CAP-ES V2 for RAC

[Version] 2.4.100.0

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Others

Exported to(language) USA(en)
[Firmware No.] D592-0011N
[File Information]
 File Name D592-0011N.exe
 File Type Module for Service
 Size 884.62 MB (927589940 byte)
 Check Sum -8Bit Sum: 0057
  -16Bit Sum(Little Endian): CDED
  -16Bit Sum(Big Endian): 896A

[Production reflection]

==========
*** Note ***
==========
[Note]

==========
*** Important Notes ***
==========
[Important Notes]

==========
*** Modification History ***
==========
[Modifications made:]
Fixed:
- The user associated billing code information may be deleted by
  task synchronization.
- User associated billing code information (.csv file) that has
  empty domain names cannot be imported.

[Modification history]

Version 2.4.000.0
Support:
- Windows Server 2016 is supported.
- SQL Server 2016 is supported.
- Windows Server 2003/2003 R2/Windows 8 are excluded as support
  environments.

Fixed:
- Update installation from v2.3 to v2.3.100 may fail.
- Offline deactivation may fail.
- When adding a group to the Group Authorization Information List
  via the Administrative Tool, [Color Copy Mode Limitation] may not
  be displayed correctly.
- The error message may not be displayed correctly when
  adding/editing a card ID with many characters.
- Duplicated or deleted cards and errors related to them may not be
  displayed correctly.

Other:
- Billing codes can be obtained from a user attribute.
- Activation method has been changed from server license to client
  access license (CAL).
- A fix for the Apache Commons FileUpload (ACF) vulnerability has
  been added.

Version V2.3.100.0
Support:
1. Support for TLS1.2 has been added.
 *The Java VM version on the device must support TLS1.2.
2. Support for SHA-2 has been added.
 *The Java VM version on the device must support SHA-2.

Fixed:
1. When editing a card ID from lowercase characters to capital
   characters, the edited ID will be deleted after saving the data.
2. Administrator privileges are assigned to users irregularly after
   task synchronization is performed.
3. When trying to newly add an external user who belongs to an

external group to an internal group via a CSV file import, the user will be deleted from the external group.
4. An authentication error will occur and no error will be recorded in CAP-ES when Task synchronization, CSV import, and Delete All Users are executed at the same time and a user tries to authenticate.

Other:
1. RSInfo has been updated.
2. A fix for the Apache Commons Collection (ACC) vulnerability has been added.

Version V2.3.000.0
Supported:
1. Support for Fire Fox ESR 38 has been added.

Fix:
1. In SSL environment, CAP-ES may not be synchronized to external authentication server.
2. If synchronization to external authentication server is performed without proxy user, Jetty may be down and the synchronization fails.
3. When LDAP authentication is performed, E00001 or E03002 error may occur.

Other:
1. Billing Code can be registered to CAP-ES.
2. CAP-ES database can be synchronized between primary and secondary server.
3. Activation site has been changed from GMP server to eDC-i server.
4. RSInfo has been updated.
5. Java version has been updated to 8.

Version 2.2.7.0
Fixed:
1. The built-in user (admin/service) can be registered as a normal user.
2. If a login user name is searched for by using capital letters, the user will not be found in the case that "Convert to Lower Case" is specified in the Login User Name settings under Registration Method in Default Settings.
3. If authentication or synchronization is performed after modifying capital/lowercase letters in the registered user's domain name, 2 users will be registered that only differ by their domain names having capital or lowercase letters. This will cause an authentication error to occur.
4. An internal user's Identification Name can be changed by modifying and importing a Group Authorization Information .csv file.
5. After a user who belongs to an external group is registered in CAP-ES and overwrite importing is performed using an Integrated Information .csv file that does not contain the user, no name

group will be registered to the user.
6. When importing an Integrated Information .csv file, the information log will be incomplete.
7. The message "Enterprise Server Module for CAP V1 Users is to be installed later" will be displayed when confirming whether "Enterprise Server Module for CAP V1 Users" is installed when installing CAP-ES v2.
8. Even if a group is deleted from CAP-ES, the Group Authorization Information List for the group will not be deleted.
9. If an Integrated Information group name is 64 characters or more, the .csv file cannot be imported.
10. The CPU usage for the CAP-ES service may become 100% because of Apache Commons File Upload library instability.
(http://mail-archives.us.apache.org/mod_mbox/www-announce/201402.mbox/%3C52F373FC.9030907@apache.org%3E).
11. If the Account Lock Threshold value set in Active Directory is the same (or less) than the domain controller number specified in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an account lock will occur if the input user's password is incorrect.
12. There is a possibility that SSL 3.0 with a CBC cipher may be decrypted by using a padding-oracle attack.
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566)
13. If multiple domains are specified for "Domain Name" in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an authentication error may occur.

Other:
1. CAP-ES outputs the following logs into the Windows Application Event log:
- The results of operating a .bat file.
- When an error occurs.
2. Delete all user information in the CAP-ES database at one time by using "UserAllDelete.bat".
3. The Card ID can be searched for via the User Display Name.
4. A message for confirming if the database is on an internal or external server will be displayed when upgrading. In the case that the database is internal, the database will be updated automatically during the CAP-ES version-up flow. In the case that the database is external, perform the "Create Database" procedure on the external server separately.
5. An attribute on an external authentication server that has multiple values can be specified in "Attribute Name Settings" for card IDs. Up to 10 values (card IDs) are supported.
6. Failover Clustering for Windows Server 2012/2012 R2 is supported.
7. The AES 128/256-bit encryption method can be used for Kerberos Authentication.
8. "SQL Server Name", "Database Instance Name", and "Database Name" can be changed via the Database Management Tool.

==========
*** Basic Information ***
==========
[Create date] 2017/06/16

[Program Name] CAP-ES V2 for RA

[Version] 2.4.100.0

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Others

Exported to(language) ASI(en)
[Firmware No.] D592-0021N
[File Information]
 File Name D592-0021N.exe
 File Type Module for Service
 Size 884.62 MB (927587593 byte)
 Check Sum -8Bit Sum: 8EAB
  -16Bit Sum(Little Endian): B522
  -16Bit Sum(Big Endian): 8489

[Production reflection]

==========
*** Note ***
==========
[Note]

==========
*** Important Notes ***
==========
[Important Notes]

==========
*** Modification History ***
==========
[Modifications made:]
Fixed:
- The user associated billing code information may be deleted by
  task synchronization.
- User associated billing code information (.csv file) that has
  empty domain names cannot be imported.

[Modification history]

Version 2.4.000.0
Support:
- Windows Server 2016 is supported.
- SQL Server 2016 is supported.
- Windows Server 2003/2003 R2/Windows 8 are excluded as support
  environments.

Fixed:
- Update installation from v2.3 to v2.3.100 may fail.
- Offline deactivation may fail.
- When adding a group to the Group Authorization Information List
  via the Administrative Tool, [Color Copy Mode Limitation] may not
  be displayed correctly.
- The error message may not be displayed correctly when
  adding/editing a card ID with many characters.
- Duplicated or deleted cards and errors related to them may not be
  displayed correctly.

Other:
- Billing codes can be obtained from a user attribute.
- Activation method has been changed from server license to client
  access license (CAL).
- A fix for the Apache Commons FileUpload (ACF) vulnerability has
  been added.

Version V2.3.100.0
Support:
1. Support for TLS1.2 has been added.
 *The Java VM version on the device must support TLS1.2.
2. Support for SHA-2 has been added.
 *The Java VM version on the device must support SHA-2.

Fixed:
1. When editing a card ID from lowercase characters to capital
   characters, the edited ID will be deleted after saving the data.
2. Administrator privileges are assigned to users irregularly after
   task synchronization is performed.
3. When trying to newly add an external user who belongs to an

external group to an internal group via a CSV file import, the user will be deleted from the external group.
4. An authentication error will occur and no error will be recorded in CAP-ES when Task synchronization, CSV import, and Delete All Users are executed at the same time and a user tries to authenticate.

Other:
1. RSInfo has been updated.
2. A fix for the Apache Commons Collection (ACC) vulnerability has been added.

Version V2.3.000.0
Supported:
1. Support for Fire Fox ESR 38 has been added.

Fix:
1. In SSL environment, CAP-ES may not be synchronized to external authentication server.
2. If synchronization to external authentication server is performed without proxy user, Jetty may be down and the synchronization fails.
3. When LDAP authentication is performed, E00001 or E03002 error may occur.

Other:
1. Billing Code can be registered to CAP-ES.
2. CAP-ES database can be synchronized between primary and secondary server.
3. Activation site has been changed from GMP server to eDC-i server.
4. RSInfo has been updated.
5. Java version has been updated to 8.

Version 2.2.7.0
Fixed:
1.The built-in user (admin/service) can be registered as a normal user.
2. If a login user name is searched for by using capital letters, the user will not be found in the case that "Convert to Lower Case" is specified in the Login User Name settings under Registration Method in Default Settings.
3. If authentication or synchronization is performed after modifying capital/lowercase letters in the registered user's domain name, 2 users will be registered that only differ by their domain names having capital or lowercase letters. This will cause an authentication error to occur.
4. An internal user's Identification Name can be changed by modifying and importing a Group Authorization Information .csv file.
5. After a user who belongs to an external group is registered in CAP-ES and overwrite importing is performed using an Integrated Information .csv file that does not contain the user, no name

group will be registered to the user.
6. When importing an Integrated Information .csv file, the information log will be incomplete.
7. The message "Enterprise Server Module for CAP V1 Users is to be installed later" will be displayed when confirming whether "Enterprise Server Module for CAP V1 Users" is installed when installing CAP-ES v2.
8. Even if a group is deleted from CAP-ES, the Group Authorization Information List for the group will not be deleted.
9. If an Integrated Information group name is 64 characters or more, the .csv file cannot be imported.
10. The CPU usage for the CAP-ES service may become 100% because of Apache Commons File Upload library instability.
(http://mail-archives.us.apache.org/mod_mbox/www-announce/201402.mbox/%3C52F373FC.9030907@apache.org%3E).
11. If the Account Lock Threshold value set in Active Directory is the same (or less) than the domain controller number specified in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an account lock will occur if the input user's password is incorrect.
12. There is a possibility that SSL 3.0 with a CBC cipher may be decrypted by using a padding-oracle attack.
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566)
13. If multiple domains are specified for "Domain Name" in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an authentication error may occur.

Other:
1. CAP-ES outputs the following logs into the Windows Application Event log:
 - The results of operating a .bat file.
 - When an error occurs.
2. Delete all user information in the CAP-ES database at one time by using "UserAllDelete.bat".
3. The Card ID can be searched for via the User Display Name.
4. A message for confirming if the database is on an internal or external server will be displayed when upgrading. In the case that the database is internal, the database will be updated automatically during the CAP-ES version-up flow. In the case that the database is external, perform the "Create Database" procedure on the external server separately.
5. An attribute on an external authentication server that has multiple values can be specified in "Attribute Name Settings" for card IDs. Up to 10 values (card IDs) are supported.
6. Failover Clustering for Windows Server 2012/2012 R2 is supported.
7. The AES 128/256-bit encryption method can be used for Kerberos Authentication.
8. "SQL Server Name", "Database Instance Name", and "Database Name" can be changed via the Database Management Tool.

==========
*** Basic Information ***
==========
[Create date] 2017/06/16

[Program Name] CAP-ES V2 for RKR

[Version] 2.4.100.0

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Others

Exported to(language) KOR(en)
[Firmware No.] D592-0031N
[File Information]
 File Name D592-0031N.exe
 File Type Module for Service
 Size 884.63 MB (927603856 byte)
 Check Sum -8Bit Sum: 77EF
  -16Bit Sum(Little Endian): A9C4
  -16Bit Sum(Big Endian): BD2B

[Production reflection]

==========
*** Note ***
==========
[Note]

==========
*** Important Notes ***
==========
[Important Notes]

==========
*** Modification History ***
==========
[Modifications made:]
Fixed:
- The user associated billing code information may be deleted by
  task synchronization.
- User associated billing code information (.csv file) that has
  empty domain names cannot be imported.

[Modification history]

Version 2.4.000.0
Support:
- Windows Server 2016 is supported.
- SQL Server 2016 is supported.
- Windows Server 2003/2003 R2/Windows 8 are excluded as support
  environments.

Fixed:
- Update installation from v2.3 to v2.3.100 may fail.
- Offline deactivation may fail.
- When adding a group to the Group Authorization Information List
  via the Administrative Tool, [Color Copy Mode Limitation] may not
  be displayed correctly.
- The error message may not be displayed correctly when
  adding/editing a card ID with many characters.
- Duplicated or deleted cards and errors related to them may not be
  displayed correctly.

Other:
- Billing codes can be obtained from a user attribute.
- Activation method has been changed from server license to client
  access license (CAL).
- A fix for the Apache Commons FileUpload (ACF) vulnerability has
  been added.

Version 2.2.7.0
Fixed:
1. The built-in user (admin/service) can be registered as a normal user.
2. If a login user name is searched for by using capital letters,
   the user will not be found in the case that "Convert to Lower
   Case" is specified in the Login User Name settings under
   Registration Method in Default Settings.
3. If authentication or synchronization is performed after modifying
   capital/lowercase letters in the registered user's domain name,
   2 users will be registered that only differ by their domain names
   having capital or lowercase letters. This will cause an
   authentication error to occur.
4. An internal user's Identification Name can be changed by

modifying and importing a Group Authorization Information .csv file.
5. After a user who belongs to an external group is registered in CAP-ES and overwrite importing is performed using an Integrated Information .csv file that does not contain the user, no name group will be registered to the user.
6. When importing an Integrated Information .csv file, the information log will be incomplete.
7. The message "Enterprise Server Module for CAP V1 Users is to be installed later" will be displayed when confirming whether "Enterprise Server Module for CAP V1 Users" is installed when installing CAP-ES v2.
8. Even if a group is deleted from CAP-ES, the Group Authorization Information List for the group will not be deleted.
9. If an Integrated Information group name is 64 characters or more, the .csv file cannot be imported.
10. The CPU usage for the CAP-ES service may become 100% because of A pache Commons File Upload library instability.
(http://mail-archives.us.apache.org/mod_mbox/www-announce/201402.mbox/%3C52F373FC.9030907@apache.org%3E).
11. If the Account Lock Threshold value set in Active Directory is the same (or less) than the domain controller number specified in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an account lock will occur if the input user's password is incorrect.
12. There is a possibility that SSL 3.0 with a CBC cipher may be decrypted by using a padding-oracle attack.
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566)
13. If multiple domains are specified for "Domain Name" in the Server Settings and Active Directory (LDAP) is specified as the authentication type, an authentication error may occur.

Other:
1. CAP-ES outputs the following logs into the Windows Application Event log:
 - The results of operating a .bat file.
 - When an error occurs.
2. Delete all user information in the CAP-ES database at one time by using "UserAllDelete.bat".
3. The Card ID can be searched for via the User Display Name.
4. A message for confirming if the database is on an internal or external server will be displayed when upgrading. In the case that the database is internal, the database will be updated automatically during the CAP-ES version-up flow. In the case that the database is external, perform the "Create Database" procedure on the external server separately.
5. An attribute on an external authentication server that has multiple values can be specified in "Attribute Name Settings" for card IDs. Up to 10 values (card IDs) are supported.
6. Failover Clustering for Windows Server 2012/2012 R2 is supported.
7. The AES 128/256-bit encryption method can be used for Kerberos Authentication.
8. "SQL Server Name", "Database Instance Name", and "Database Name" can be changed via the Database Management Tool.