

Resetting configuration and switching deployment server (for deployment client)

Graeme DAVEY David Bevin Billy ADHI Bruce MELLOWS Suneetha THATHA XingXing SONG Zhen ZHAO

Updated since Rio Build 8.0.0.2009

Once a relationship is established between deployment client and deployment server via deployment configurator, the following changes will be made and settings retained even after Citect program is to be uninstalled.

1. On the deployment server,
 1. Deployment Database, FileRepository and Temp directory (*C:\ProgramData\Schneider Electric\Citect SCADA 2016\Deployment\Server*)
 2. SE.Asb.Deployment.Server.WindowsService.exe.config (*C:\ProgramData\Schneider Electric\Citect SCADA 2016\Config*)
 3. Port binding and URLACL (via NetSH)
 4. Certificates (CA, Signing and Binding via Certificate management console)
 5. Role groups (Asb.Deployment.AdminRole, Asb.Deployment.DeployRole, Asb.Deployment.ReadRole and Asb.Deployment.UploadRole)
 6. ADS secrets (*C:\Users\ArchestrADataStore\AppData\Roaming\Schneider Electric\ArchestrA Data Store*)
 7. Firewall rule exception (if applicable)
2. On the deployment client
 1. Deployment Database, Cache and Projects (*C:\ProgramData\Schneider Electric\Citect SCADA 2016\Deployment\Client*)
 2. SE.Asb.Deployment.Node.WindowsService.exe.config (*C:\ProgramData\Schneider Electric\Citect SCADA 2016\Config*)
 3. Port binding and URLACL (via NetSH)
 4. Certificates (CA public key, Signing and Binding via Certificate management console)
 5. ADS secrets (*C:\Users\ArchestrADataStore\AppData\Roaming\Schneider Electric\ArchestrA Data Store*)
 6. Firewall rule exception (if applicable)

Reset settings of Deployment server and node

By performing the following, we will **reset the server to a fresh install.**

1. Stop the service Start -> Run -> net stop "Citect Deployment Server Service"
2. Delete the certificates from store
 1. Certificates - Local Computer - Trusted Root Certification - Certificate, Citect Deployment CA
 2. Certificates - Local Computer - Personal - Certificates - Citect Deployment server code signing
 3. Certificates - Local Computer - Personal - Certificates - Citect Deployment server code binding (if exist)
3. Delete the following file *C:\ProgramData\Schneider Electric\Citect SCADA 2016\Config\SE.Asb.Deployment.Server.WindowsService.exe.config*
4. Delete port binding by executing the following command in command prompt under elevated administrator mode
 1. netsh http delete sslcert 0.0.0.0:443
 2. netsh http delete urlacl https://+:443/api/asb/DeploymentServer/
5. Delete directory and its contents *C:\ProgramData\Schneider Electric\Citect SCADA 2016\Deployment\Server*
6. To reset ADS secrets
 1. Delete directory and its contents *C:\Users\ArchestrADataStore\AppData\Roaming\Schneider Electric\ArchestrA Data Store*
 2. Restart service "ArchestrA Data Store"
 1. Stop the service Start -> Run -> net stop "ArchestrA Data Store"
 2. Start the service Start -> Run -> net start "ArchestrA Data Store"
7. Remove firewall exception rule
8. Remove following role groups
 1. Asb.Deployment.AdminRole
 2. Asb.Deployment.DeployRole
 3. Asb.Deployment.ReadRole
 4. Asb.Deployment.UploadRole
9. Once the server is reset, deployment clients will no longer be able to establish a connection with it.

By performing the following, we will **reset the client to a fresh install.**

1. Stop the service Start -> Run -> net stop "Citect Deployment Client Service"
2. Delete the certificates from store (If both server and client is running on same machine, skip this step if you do not intend on resetting the server)
 1. Certificates - Local Computer - Trusted Root Certification - Certificate, Citect Deployment CA
 2. Certificates - Local Computer - Personal - Certificates - Citect Deployment server code signing
 3. Certificates - Local Computer - Personal - Certificates - Citect Deployment agent port binding (if exist)
3. Delete the following file *C:\ProgramData\Schneider Electric\Citect SCADA 2016\Config\SE.Asb.Deployment.Node.WindowsService.exe.config*
4. Delete port binding by executing the following command in command prompt under elevated administrator mode (If both server and client is running on same machine, skip this step if you do not intend on resetting the server)
 1. netsh http delete sslcert 0.0.0.0:443
 2. netsh http delete urlacl https://+:443/api/asb/DeploymentNode/
5. Delete directory and its contents *C:\ProgramData\Schneider Electric\Citect SCADA 2016\Deployment\Client*
6. To reset ADS secrets
 1. Delete directory and its contents *C:\Users\ArchestrADataStore\AppData\Roaming\Schneider Electric\ArchestrA Data Store*

2. Restart service "ArchestrA Data Store"
 1. Stop the service Start -> Run -> net stop "ArchestrA Data Store"
 2. Start the service Start -> Run -> net start "ArchestrA Data Store"
7. Remove firewall exception rule
8. Resetting the agent does not remove the device record on the deployment server.