NOVEMBER 2022

Secured Data Communication in AVEVA™ System Platform

Powered by System Management Server

Presented By: Raghu Kanchanapally & Jerry Lau

AVEVA

Agenda

Platform Common Services

System Management Server

Secured Suitelink communication

Secured MX communication

Secured HCAL-HCAP communication

SMS Certificate Management

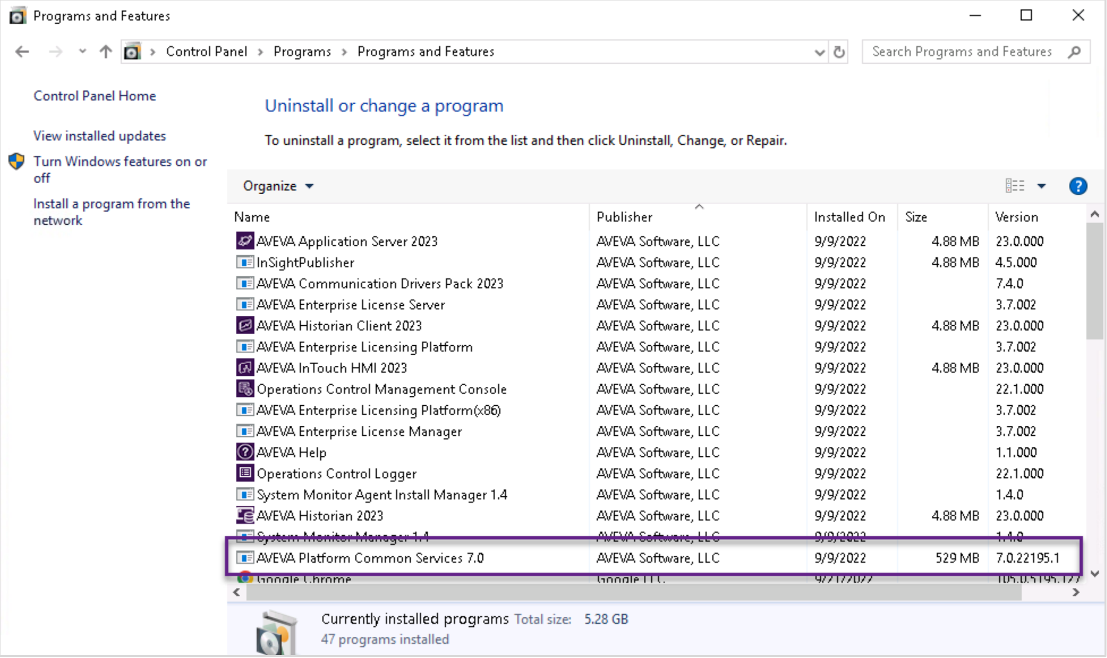
Microsoft DCOM Hardening

Troubleshooting

Platform Common Services (PCS)

Overview

- A common framework for data exchange between nodes running AVEVA products
- Formerly known as ArchestrA Service Bus (ASB)
- Based on the service-oriented architecture
- Allows different AVEVA products to be highly interoperable but still remains loosely coupled
- Backbone of the runtime data exchange, predominantly invisible to the users
- Independent of System Platform but gets automatically installed with System Platform
- Can be installed standalone as well (Ex: Recipe Manager Plus uses the standalone PCS)
- First shipped with System Platform 2012 R2



Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
AVEVA Application Server 2023	AVEVA Software, LLC	9/9/2022	4.88 MB	23.0.000
InSightPublisher	AVEVA Software, LLC	9/9/2022	4.88 MB	4.5.000
AVEVA Communication Drivers Pack 2023	AVEVA Software, LLC	9/9/2022		7.4.0
AVEVA Enterprise License Server	AVEVA Software, LLC	9/9/2022		3.7.002
AVEVA Historian Client 2023	AVEVA Software, LLC	9/9/2022	4.88 MB	23.0.000
AVEVA Enterprise Licensing Platform	AVEVA Software, LLC	9/9/2022		3.7.002
AVEVA InTouch HMI 2023	AVEVA Software, LLC	9/9/2022	4.88 MB	23.0.000
Operations Control Management Console	AVEVA Software, LLC	9/9/2022		22.1.000
AVEVA Enterprise Licensing Platform(x86)	AVEVA Software, LLC	9/9/2022		3.7.002
AVEVA Enterprise License Manager	AVEVA Software, LLC	9/9/2022		3.7.002
AVEVA Help	AVEVA Software, LLC	9/9/2022		1.1.000
Operations Control Logger	AVEVA Software, LLC	9/9/2022		22.1.000
System Monitor Agent Install Manager 1.4	AVEVA Software, LLC	9/9/2022		1.4.0
AVEVA Historian 2023	AVEVA Software, LLC	9/9/2022	4.88 MB	23.0.000
System Monitor Manager 1.4	AVEVA Software, LLC	9/9/2022		1.4.0
AVEVA Platform Common Services 7.0	AVEVA Software, LLC	9/9/2022	529 MB	7.0.22195.1
Google Chrome	Google LLC	9/17/2022		105.0.5195.127

Currently installed programs Total size: 5.28 GB
47 programs installed

Platform Common Services (PCS)

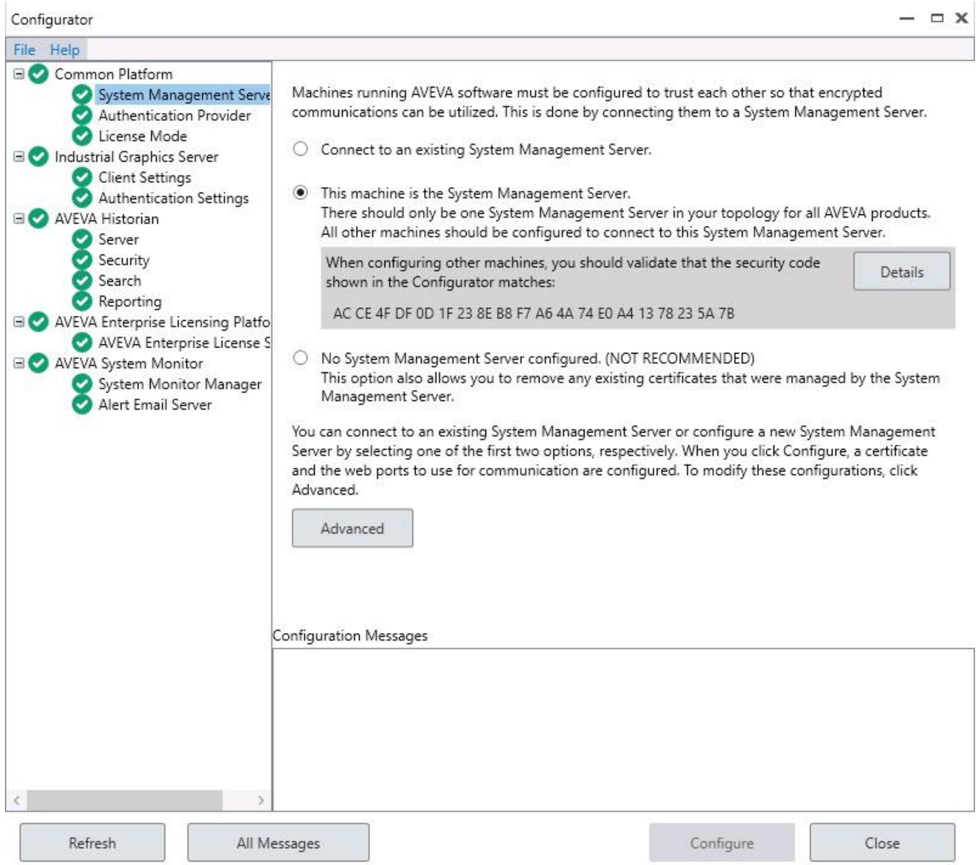
History

ASB\PCS Version	System Platform Version
2.0	SP 2014 R2
3.0	SP 2014 R2 P01
4.0	SP 2014 R2 SP1
4.1	SP 2017
4.2	SP 2017 U1
4.2.2	SP 2017 U2
4.3	SP 2017 U3
4.4.1	SP 2020
4.5.1	SP 2020 R2
7.0	SP 2023

System Management Server (SMS)

Overview

- A component of the Platform Common Services
- Provides the support for TLS 1.2 protocol for secured communication between nodes
- Acts as a certificate authority and distributes the certificates to the client nodes (only for auto generated certificates)
- Responsible for registering the new devices
- Configured through a Plug-In in the Configurator application
- All the nodes must be connected to the same SMS
- SMS node in the network is automatically discovered, if not it can be entered manually in the configurator



Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.

○ Connect to an existing System Management Server.

● This machine is the System Management Server.
There should only be one System Management Server in your topology for all AVEVA products.
All other machines should be configured to connect to this System Management Server.

When configuring other machines, you should validate that the security code shown in the Configurator matches:

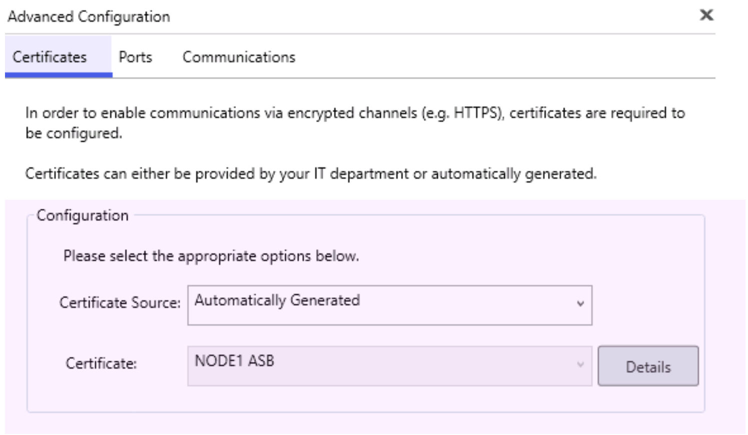
AC CE 4F DF 0D 1F 23 8E B8 F7 A6 4A 74 E0 A4 13 78 23 5A 7B

○ No System Management Server configured. (NOT RECOMMENDED)
This option also allows you to remove any existing certificates that were managed by the System Management Server.

You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click Advanced.

System Management Server (SMS)

Advanced Configuration



In order to enable communications via encrypted channels (e.g. HTTPS), certificates are required to be configured.

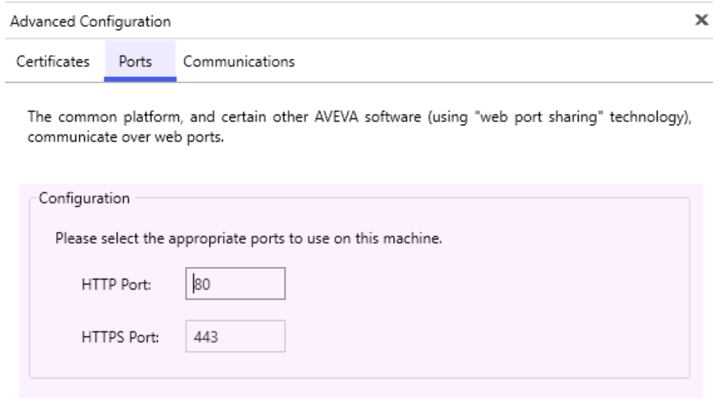
Certificates can either be provided by your IT department or automatically generated.

Configuration

Please select the appropriate options below.

Certificate Source: Automatically Generated

Certificate: NODE1 ASB



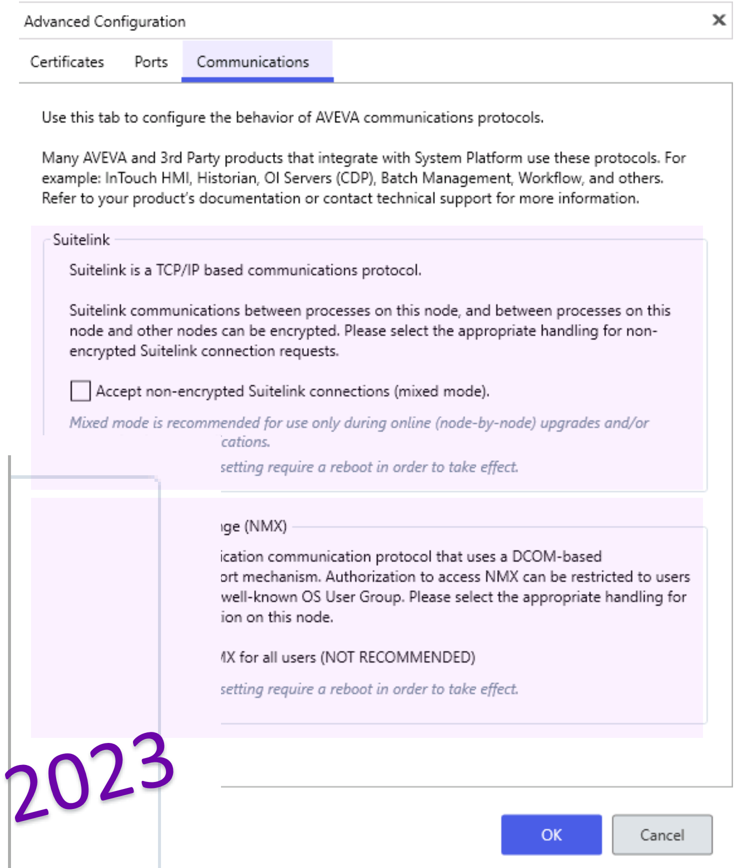
The common platform, and certain other AVEVA software (using "web port sharing" technology), communicate over web ports.

Configuration

Please select the appropriate ports to use on this machine.

HTTP Port: 80

HTTPS Port: 443



Use this tab to configure the behavior of AVEVA communications protocols.

Many AVEVA and 3rd Party products that integrate with System Platform use these protocols. For example: InTouch HMI, Historian, OI Servers (CDP), Batch Management, Workflow, and others. Refer to your product's documentation or contact technical support for more information.

Suitelink

Suitelink is a TCP/IP based communications protocol.

Suitelink communications between processes on this node, and between processes on this node and other nodes can be encrypted. Please select the appropriate handling for non-encrypted Suitelink connection requests.

☐ Accept non-encrypted Suitelink connections (mixed mode).

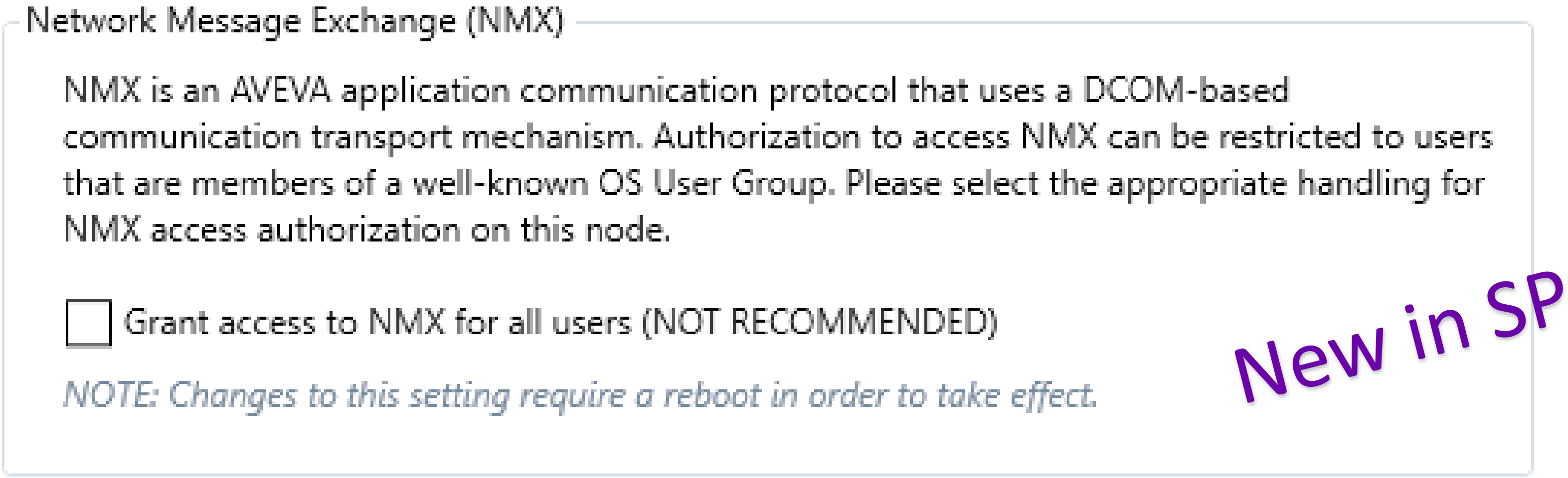
Mixed mode is recommended for use only during online (node-by-node) upgrades and/or
cations.
setting require a reboot in order to take effect.

ıge (NMX)

ication communication protocol that uses a DCOM-based
ort mechanism. Authorization to access NMX can be restricted to users
well-known OS User Group. Please select the appropriate handling for
ion on this node.

ſX for all users (NOT RECOMMENDED)

setting require a reboot in order to take effect.



Network Message Exchange (NMX)

NMX is an AVEVA application communication protocol that uses a DCOM-based communication transport mechanism. Authorization to access NMX can be restricted to users that are members of a well-known OS User Group. Please select the appropriate handling for NMX access authorization on this node.

☐ Grant access to NMX for all users (NOT RECOMMENDED)

NOTE: Changes to this setting require a reboot in order to take effect.

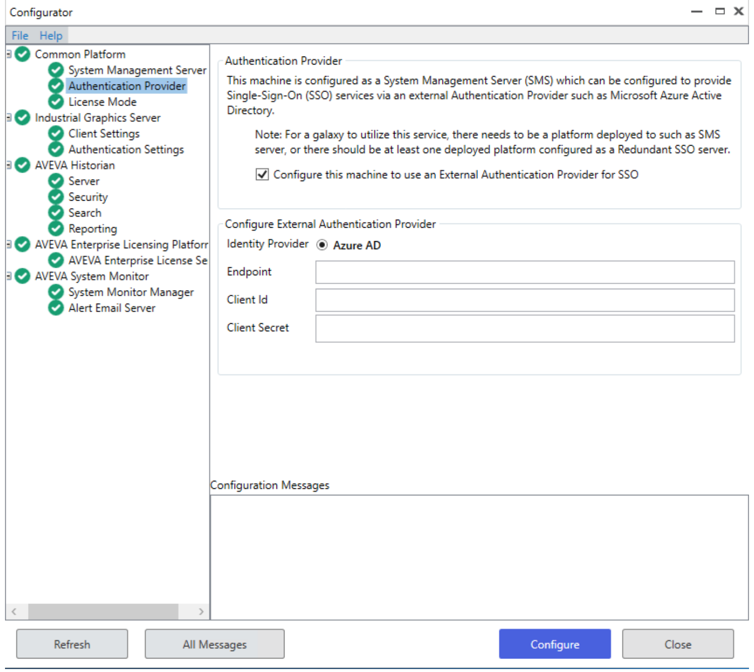
New in SP 2023

Platform Common Services (PCS)

System Management Server as an Authentication Provider

- An SMS Server Node can act as an Authentication Provider to provide Single-Sign-On services via an external authentication provider such as Microsoft Azure Active Directory

- One of the clients can be configured as a redundant Authentication Provider to provide Single-Sign-On services



Authentication Provider

This machine is configured as a System Management Server (SMS) which can be configured to provide Single-Sign-On (SSO) services via an external Authentication Provider such as Microsoft Azure Active Directory.

Note: For a galaxy to utilize this service, there needs to be a platform deployed to such as SMS server, or there should be at least one deployed platform configured as a Redundant SSO server.

☑ Configure this machine to use an External Authentication Provider for SSO

Configure External Authentication Provider

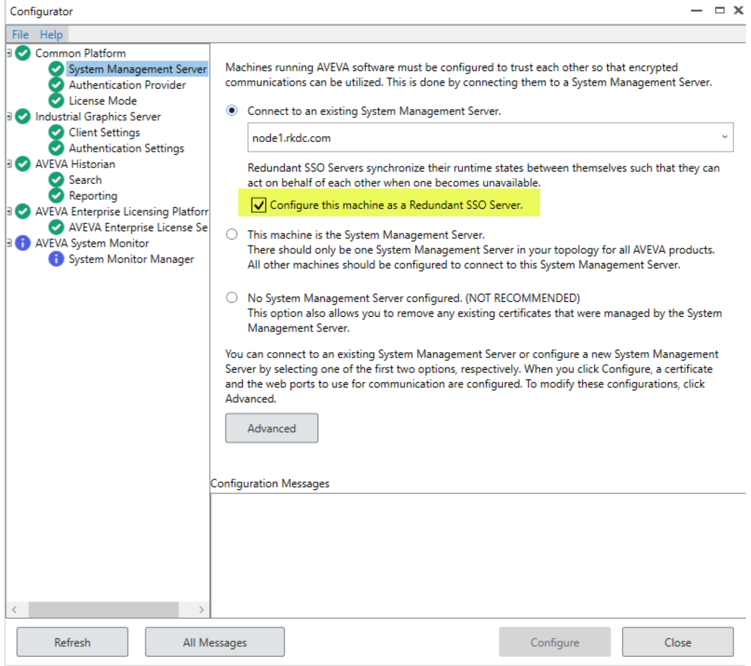
Identity Provider ● Azure AD

Endpoint

Client Id

Client Secret

Configuration Messages



Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.

● Connect to an existing System Management Server.

node1.rkdc.com

Redundant SSO Servers synchronize their runtime states between themselves such that they can act on behalf of each other when one becomes unavailable.

☑ Configure this machine as a Redundant SSO Server.

○ This machine is the System Management Server.
There should only be one System Management Server in your topology for all AVEVA products.
All other machines should be configured to connect to this System Management Server.

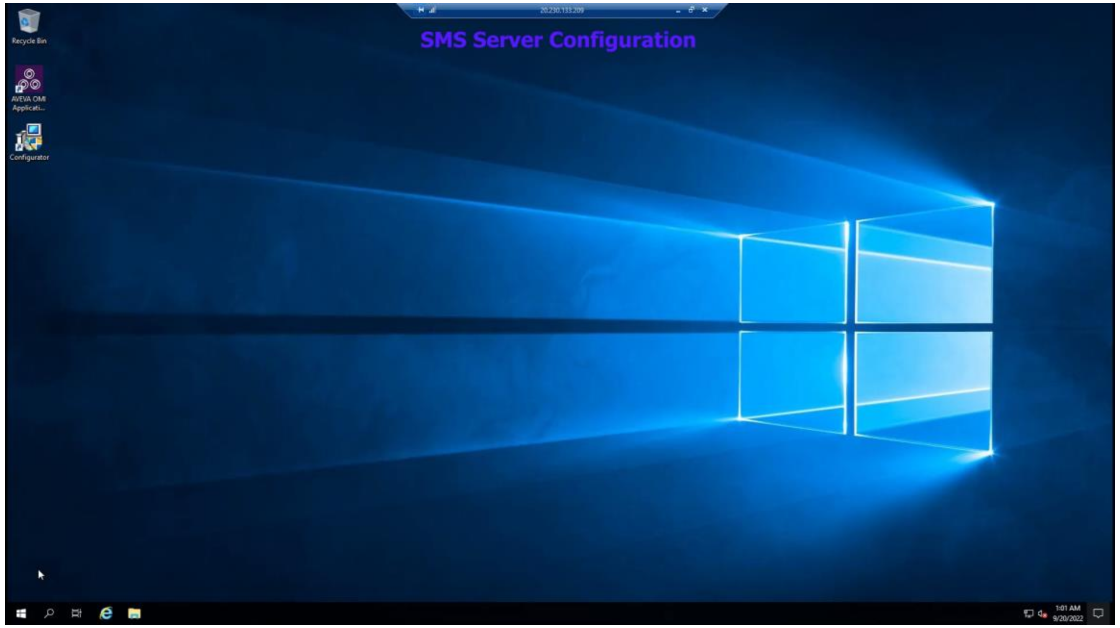
○ No System Management Server configured. (NOT RECOMMENDED)
This option also allows you to remove any existing certificates that were managed by the System Management Server.

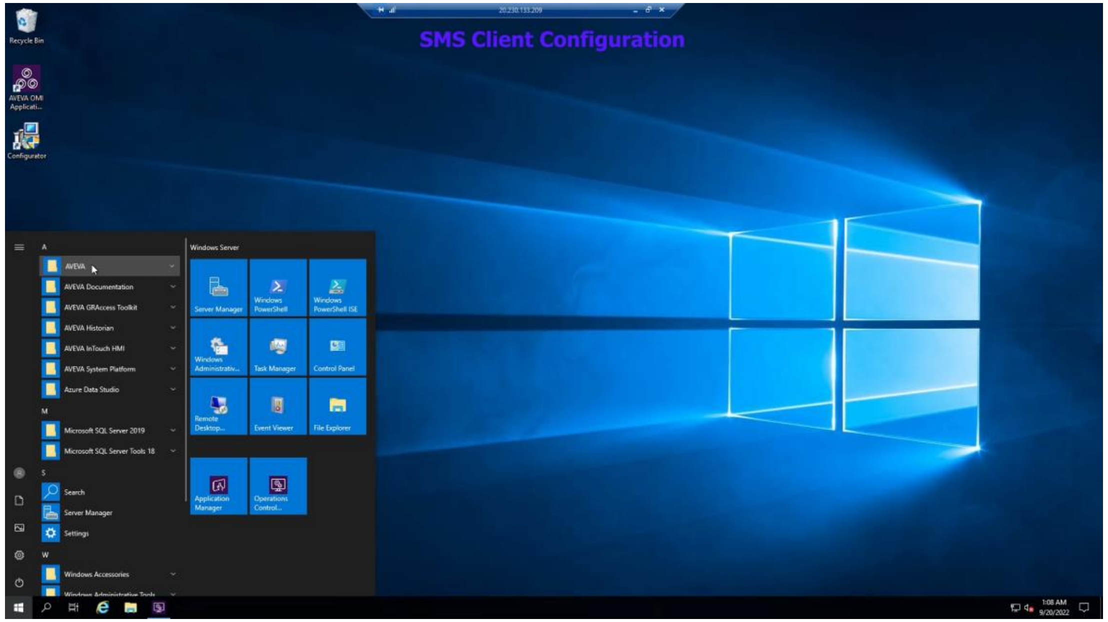
You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click Advanced.

Configuration Messages

System Management Server Configuration

Server and Client Demo



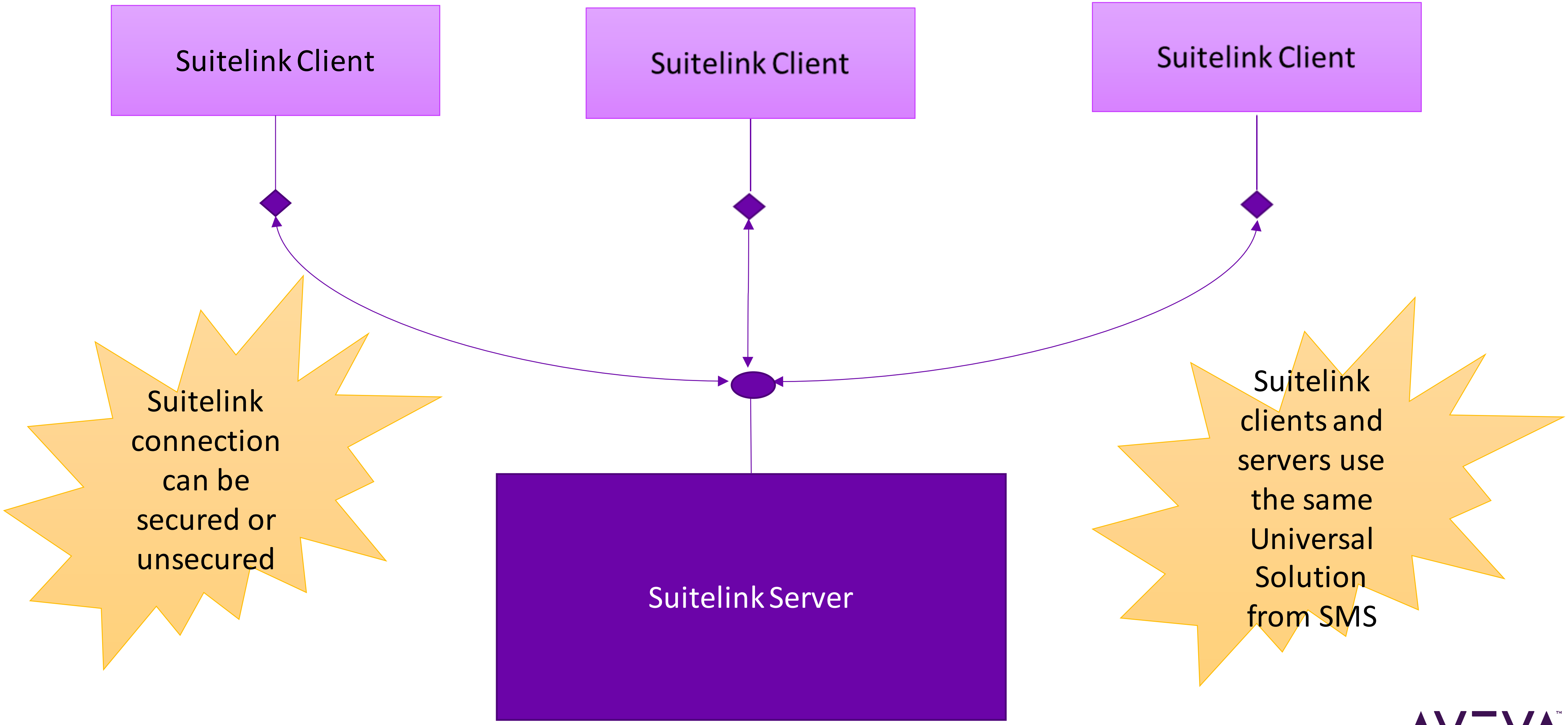


Secured Suitelink Communication

Overview

- A lightweight protocol used for high performance data transport for data items (VTQ)
- Implemented with TCP on port 5413
- Based on client-server technology for application connectivity on the network
- Drop-in replacement or upgrade without requiring the client\server applications to recompile
- Secured Suitelink encrypts the communication channel between client and server
- Encryption is achieved through the certificates provided by SMS
- Suitelink clients and servers download the Universal Solution from SMS to enable secure communication

Suitelink Architecture



Suitelink Client

Suitelink Client

Suitelink Client

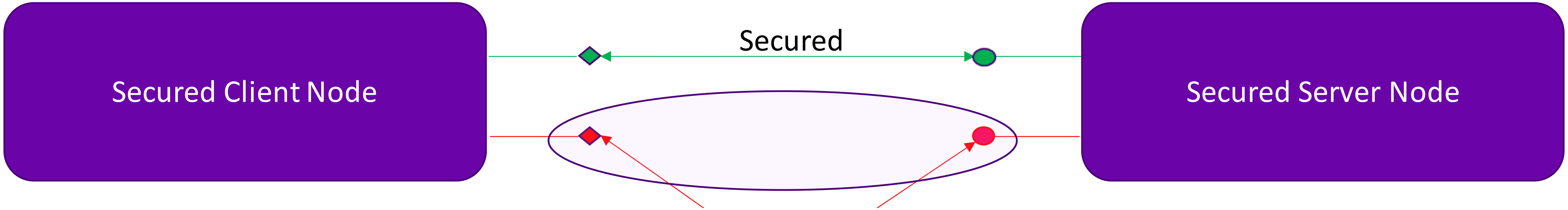
Suitelink Server

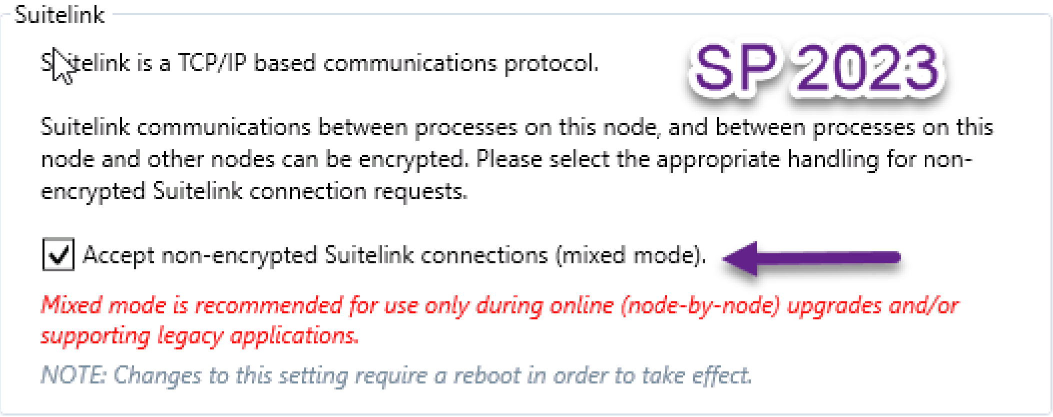
Suitelink connection can be secured or unsecured

Suitelink clients and servers use the same Universal Solution from SMS

Secure Suitelink Communication

Interoperability of legacy and secured Suitelink





Suitelink

Suitelink is a TCP/IP based communications protocol.

Suitelink communications between processes on this node, and between processes on this node and other nodes can be encrypted. Please select the appropriate handling for non-encrypted Suitelink connection requests.

☑ Accept non-encrypted Suitelink connections (mixed mode).

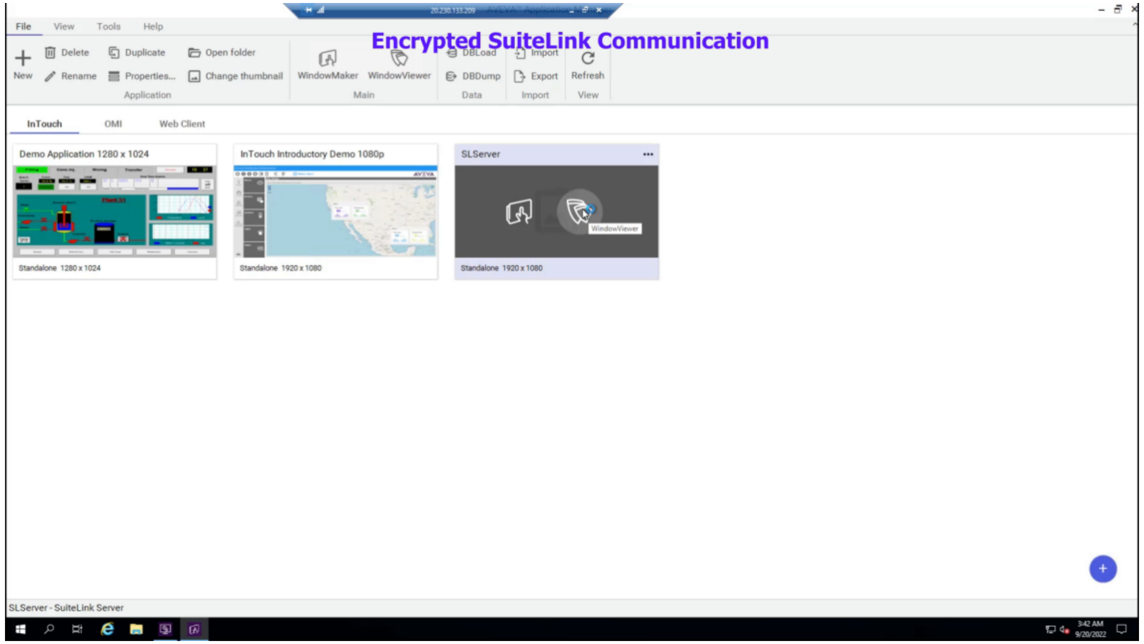
Mixed mode is recommended for use only during online (node-by-node) upgrades and/or supporting legacy applications.

NOTE: Changes to this setting require a reboot in order to take effect.

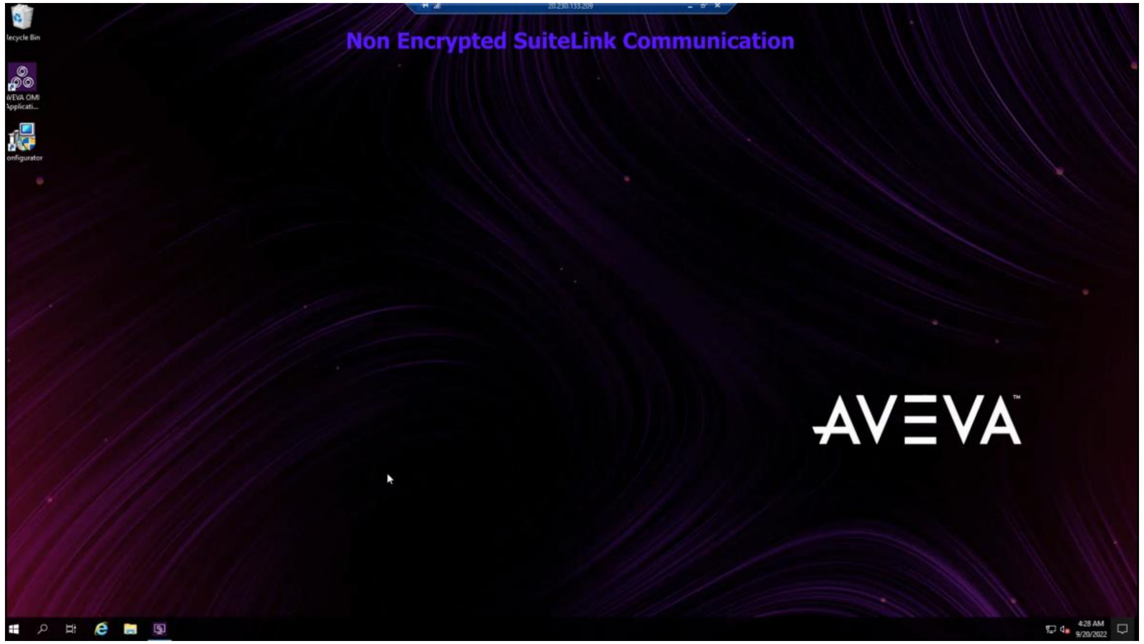
Legacy Client Node

Legacy Server Node

Secured Suitelink vs. Unsecured Suitelink Demo



Encrypted SuiteLink Communication



Non Encrypted SuiteLink Communication

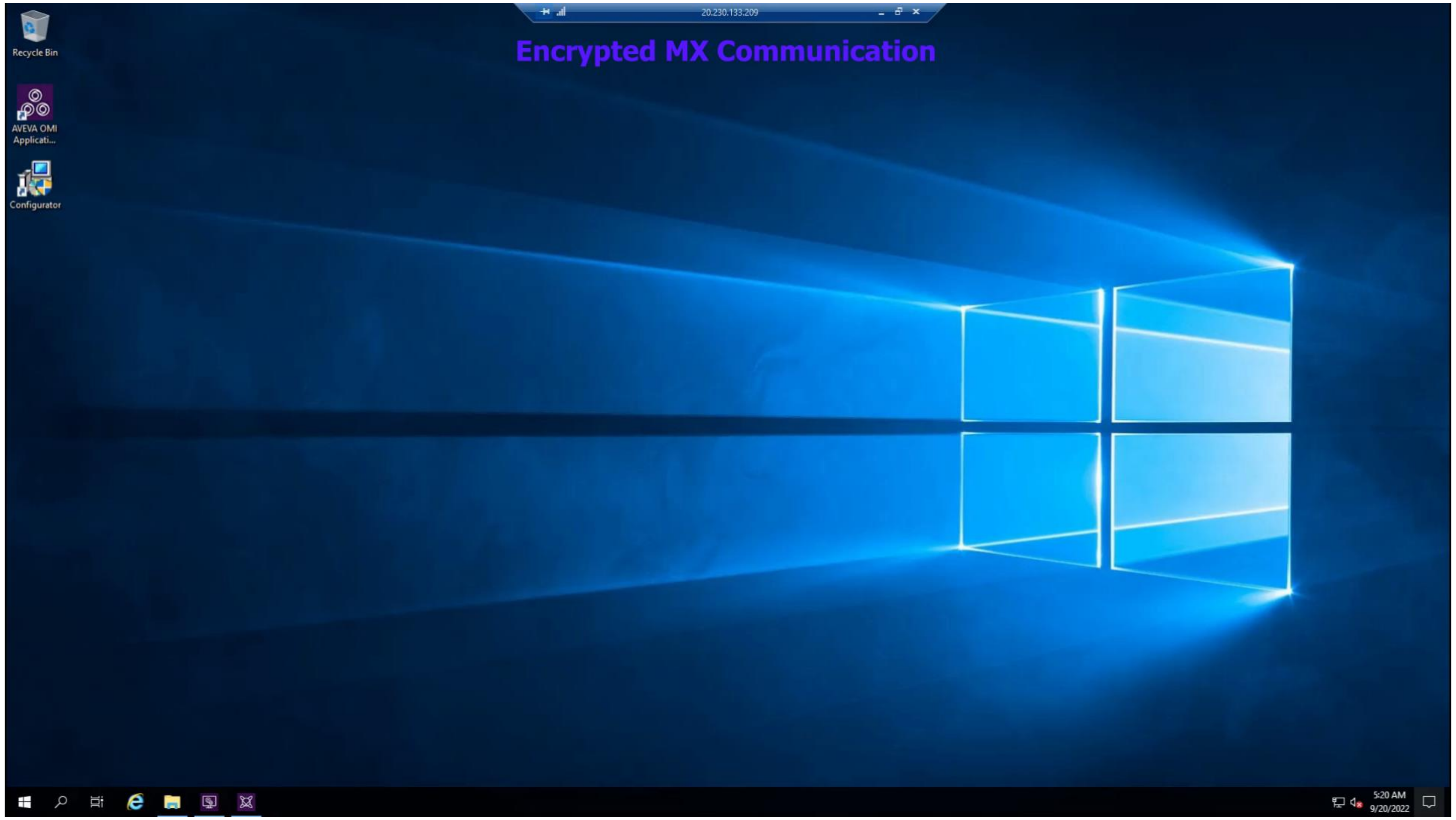
Secured MX Communication

Overview

- Message Exchange (LMX\NMX) is a protocol for Data Exchange between Application Server Runtime Nodes
- LMX is for Local Message Exchange and NMX is for Network Message Exchange
- MessageChannel is the component that connects 2 different Application Server Nodes for NMX
- MX messages are exchanged over MessageChannel for get\set of Runtime attribute data
- MessageChannel is secured with the certificate provided by SMS for secured communication

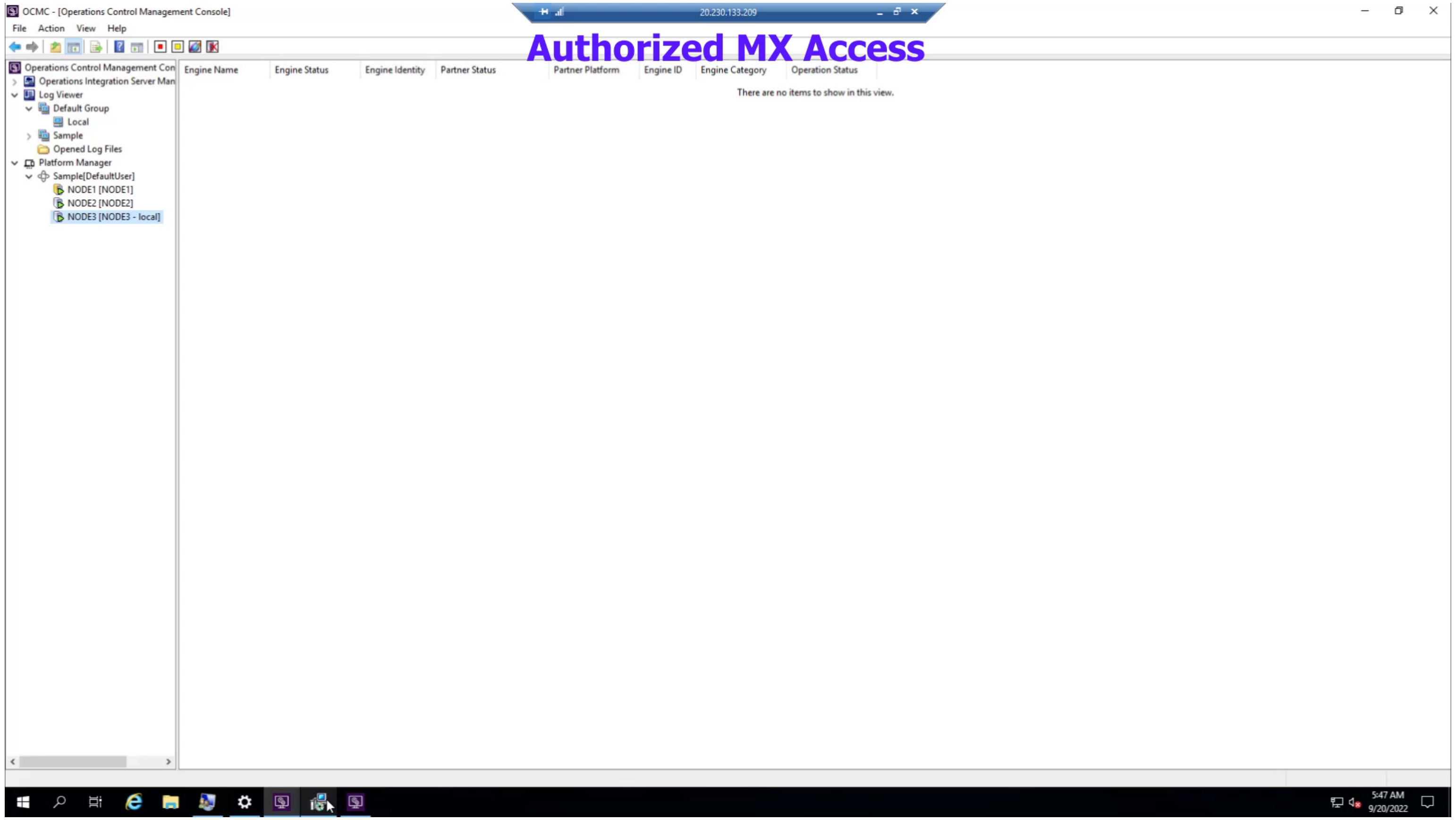
Secured MX Communication

Demo



Authorized MX Access

Demo



Engine Name	Engine Status	Engine Identity	Partner Status	Partner Platform	Engine ID	Engine Category	Operation Status

There are no items to show in this view.

Secured HCAL-HCAP Communication

Overview

- HCAL (aahClientCommon) is a client-side component used by clients (like Application Engine, Historian, SDK etc…) to establish connection with the Historian
- HCAP (aahClientAccessPoint) is a server-side component of Historian which accepts the connections from the clients
- HCAL-HCAP communication is secured when both the server node (Historian) and client node (typically Application Server Runtime Node) are configured with the same SMS
- HCAP maintains both secure and unsecure endpoints
- HCAL with fallback to unsecured connection if server side certificate cannot be validated or secured endpoint cannot be reached

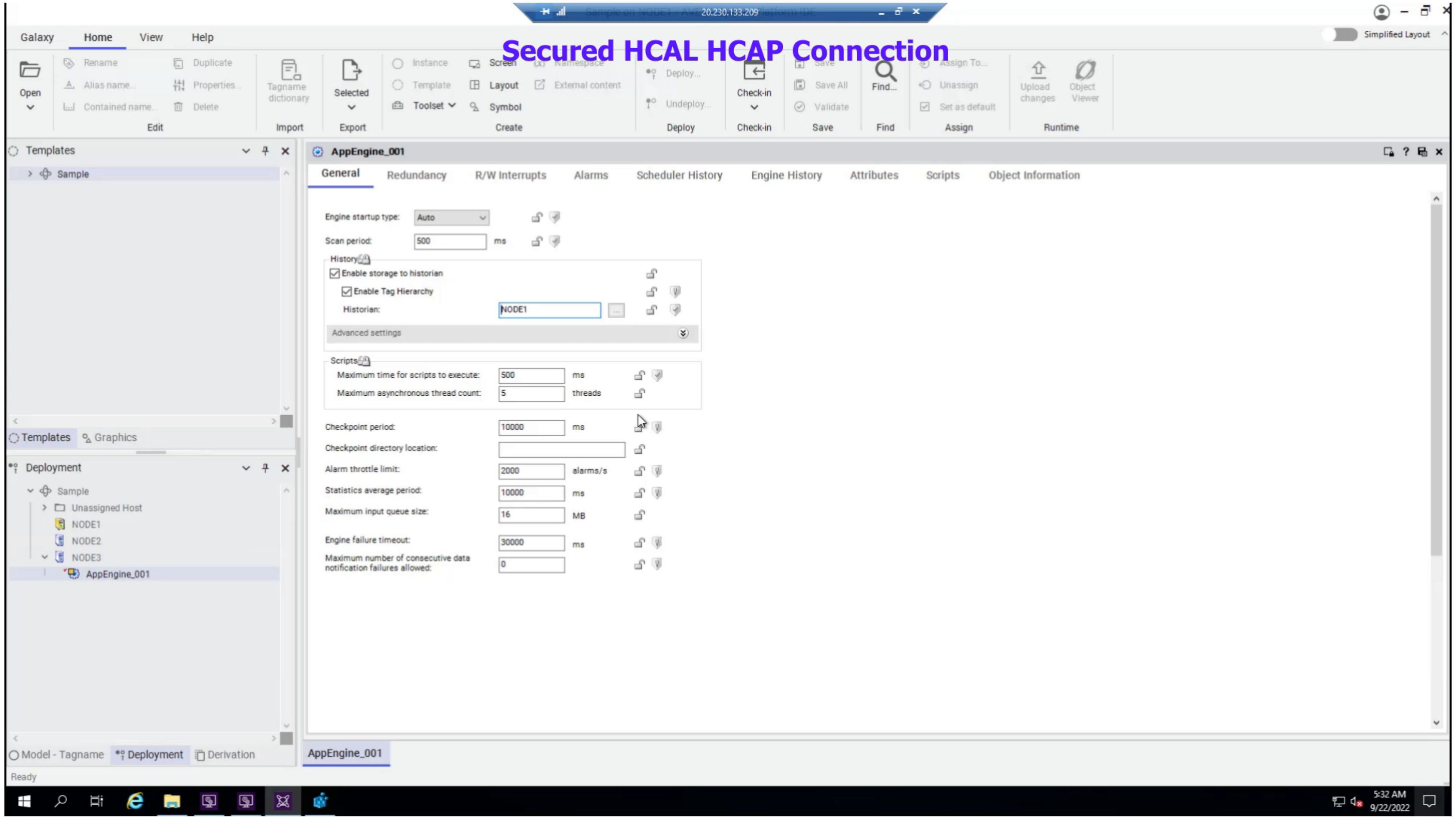
Secured HCAL-HCAP Communication

Secured HCAL-HCAP connections

- Tier-1 to Tier-2 replication
- Historian Configuration Service to remote IDAS node
- Remote IDAS to Historian
- Historian SDK application to remote Historian
- Application Engine to remote Historian
- Application Engine StoreForward to Stand-By Application Engine StoreForward storage
- Local HCAL to local HCAP is NOT secured as it is on the same node

Secured HCAL-HCAP Demo

Application Server Engine and Historian Tiered Replication



Secured HCAL HCAP Connection

AppEngine_001

Engine startup type: Auto

Scan period: 500 ms

History

☑ Enable storage to historian

☑ Enable Tag Hierarchy

Historian: NODE1

Scripts

Maximum time for scripts to execute: 500 ms

Maximum asynchronous thread count: 5 threads

Checkpoint period: 10000 ms

Checkpoint directory location:

Alarm throttle limit: 2000 alarms/s

Statistics average period: 10000 ms

Maximum input queue size: 16 MB

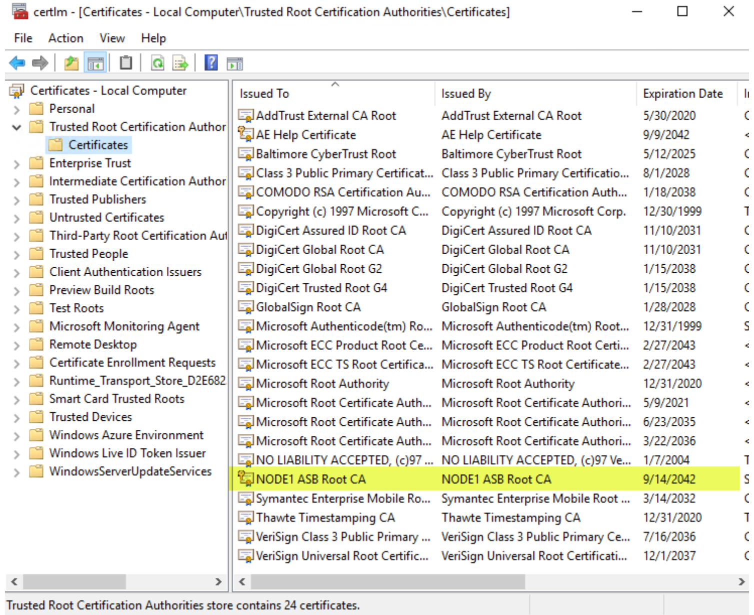
Engine failure timeout: 30000 ms

Maximum number of consecutive data notification failures allowed: 0

System Management Server

Certificate management details

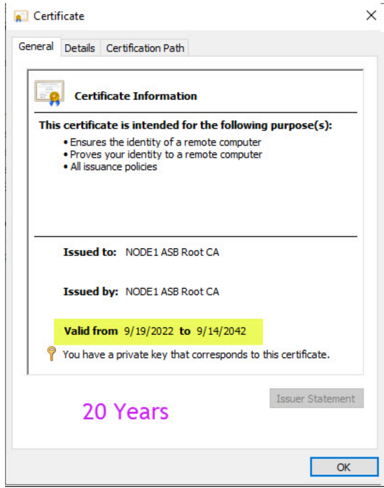
- Certificates can be managed through Certificate Manager (Certmgr.msc) Application
- Certificates can be auto generated by SMS or managed by IT
- IT managed certificates need to be manually installed on each node
- Auto generated intermediate and root certificates have a validity of 20 years
- Auto generated binding certificate has a validity of 2 years
- Watchdog Service monitors the validity of auto generated certificates and instructs the ArchestrA Certificate Renewal Service to renew automatically


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help

- Certificates - Local Computer
  - Personal
  - Trusted Root Certification Author
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Author
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Aut
  - Trusted People
  - Client Authentication Issuers
  - Preview Build Roots
  - Test Roots
  - Microsoft Monitoring Agent
  - Remote Desktop
  - Certificate Enrollment Requests
  - Runtime_Transport_Store_D2E682
  - Smart Card Trusted Roots
  - Trusted Devices
  - Windows Azure Environment
  - Windows Live ID Token Issuer
  - WindowsServerUpdateServices

Issued To	Issued By	Expiration Date
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
AE Help Certificate	AE Help Certificate	9/9/2042
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038
GlobalSign Root CA	GlobalSign Root CA	1/28/2028
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	2/27/2043
Microsoft Root Authority	Microsoft Root Authority	12/31/2020
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004
NODE1 ASB Root CA	NODE1 ASB Root CA	9/14/2042
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	12/1/2037

Trusted Root Certification Authorities store contains 24 certificates.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- All issuance policies

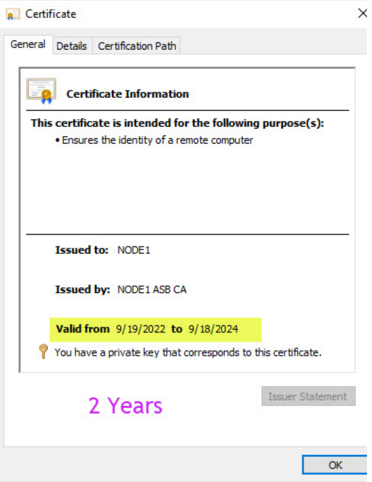
Issued to: NODE1 ASB Root CA

Issued by: NODE1 ASB Root CA

Valid from 9/19/2022 **to** 9/14/2042

You have a private key that corresponds to this certificate.

20 Years



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: NODE1

Issued by: NODE1 ASB CA

Valid from 9/19/2022 **to** 9/18/2024

You have a private key that corresponds to this certificate.

2 Years

System Management Server

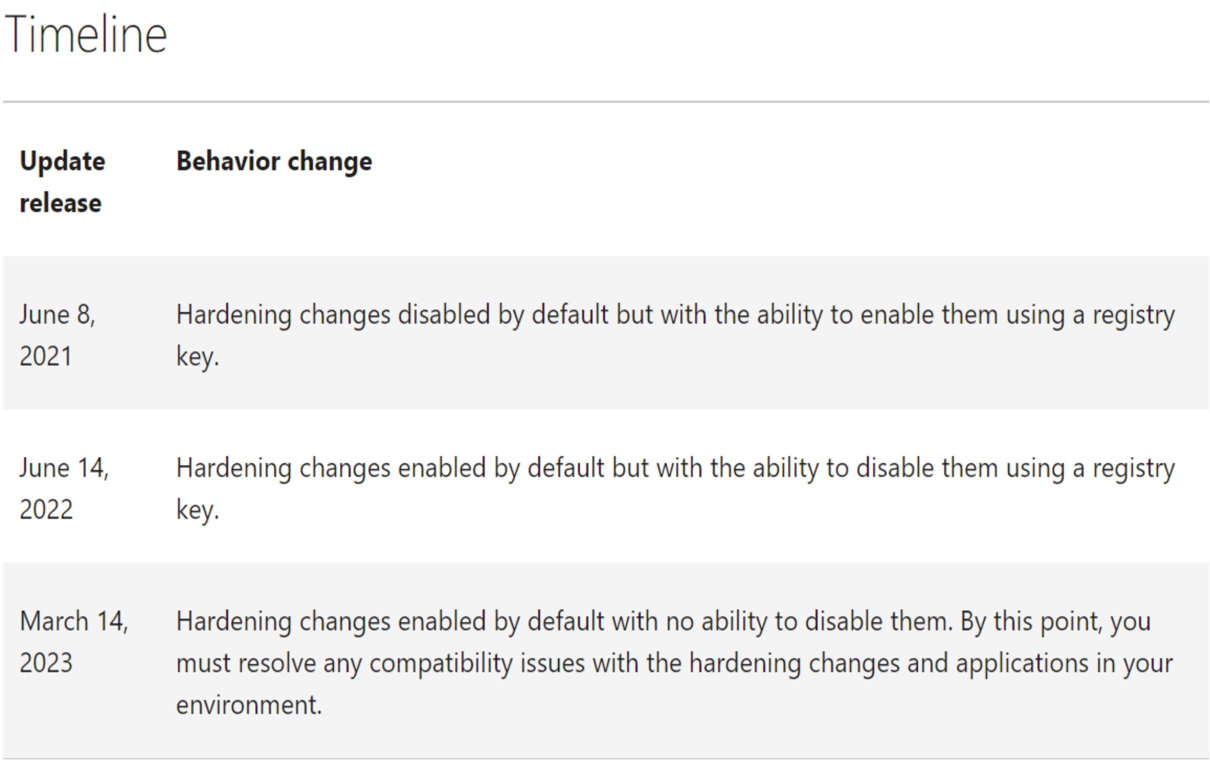
What happens if System Management Server goes down?

- No impact on runtime data exchange between the nodes
- Nodes will continue to use already established secured communication channels
- Nodes can also create new secured communication channels until the certificate expires
- Configuring a new node with “Connect to an existing SMS” option will fail
- No impact to Single-Sign-On (SSO) functionality if the Redundant Single-Sign-On (SSO) Server is configured
- Refer to Tech Note 10251 for more details

Microsoft DCOM Hardening

AVEVA's response

- More details can be found in Microsoft KB 5004442 article :
  - KB 5004442 Link
- AVEVA's response can be found in Tech Alert TA000032813 :
  - TA000032813 Link
- As of now, the Tech Alert is still work in progress, please subscribe to the Tech Alert in AVEVA Support Web Site to get notified of latest updates



Timeline

Update release	Behavior change
June 8, 2021	Hardening changes disabled by default but with the ability to enable them using a registry key.
June 14, 2022	Hardening changes enabled by default but with the ability to disable them using a registry key.
March 14, 2023	Hardening changes enabled by default with no ability to disable them. By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment.

Troubleshooting

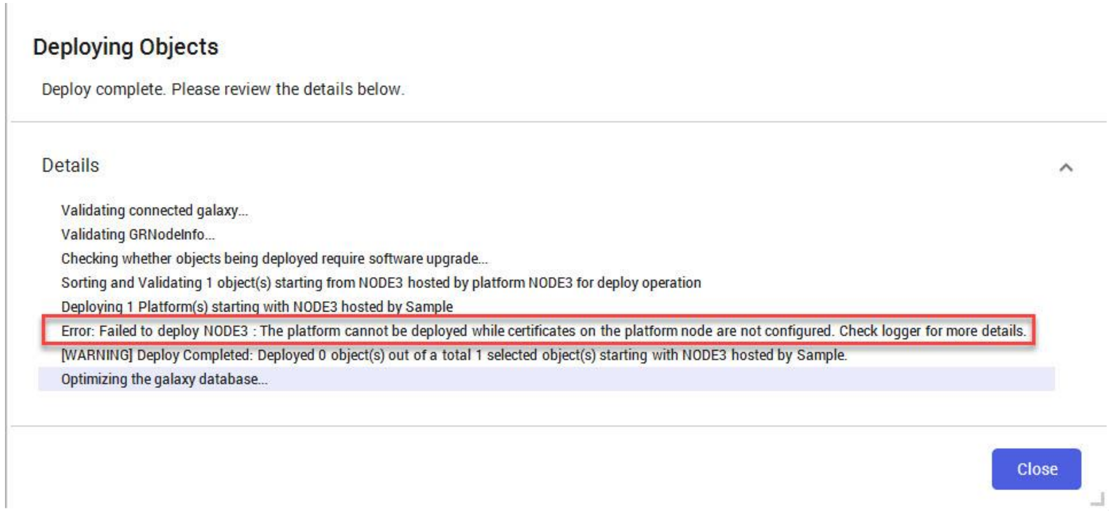
Platform Deploy Failure

Problem:

If the runtime node is not configured for System Management Server (SMS) or if it is not configured to point to the same SMS as GR Node, a platform cannot be deployed to the Runtime Node

Solution:

To avoid the problem, ensure that runtime node is configured for SMS and ensure that it is configured to point to the same SMS server as that of the GR Node

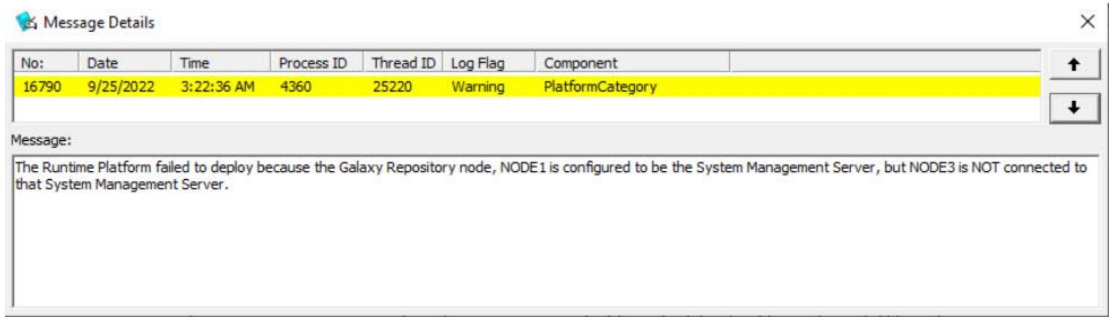


Deploying Objects

Deploy complete. Please review the details below.

Details

```
Validating connected galaxy...
Validating GRNodeInfo...
Checking whether objects being deployed require software upgrade...
Sorting and Validating 1 object(s) starting from NODE3 hosted by platform NODE3 for deploy operation
Deploying 1 Platform(s) starting with NODE3 hosted by Sample
Error: Failed to deploy NODE3 : The platform cannot be deployed while certificates on the platform node are not configured. Check logger for more details.
[WARNING] Deploy Completed: Deployed 0 object(s) out of a total 1 selected object(s) starting with NODE3 hosted by Sample.
Optimizing the galaxy database...
```



Message Details

No:	Date	Time	Process ID	Thread ID	Log Flag	Component
16790	9/25/2022	3:22:36 AM	4360	25220	Warning	PlatformCategory

Message:

The Runtime Platform failed to deploy because the Galaxy Repository node, NODE1 is configured to be the System Management Server, but NODE3 is NOT connected to that System Management Server.

Troubleshooting

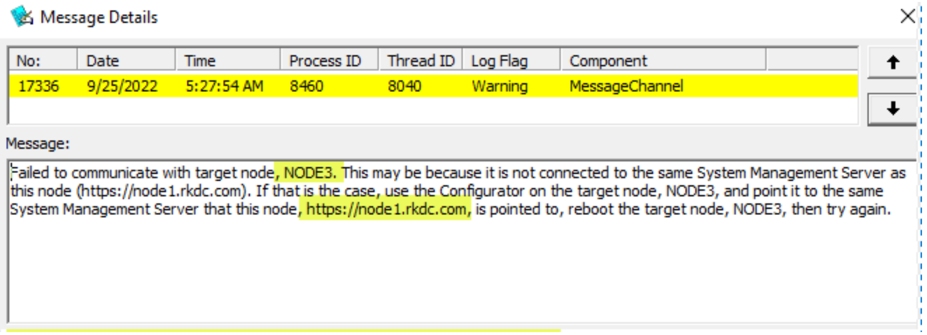
Node to Node Communication Issues

Problem:

Even after both the platform nodes pointing to the same System Management Server, the SMC Logger may report a warning that the node failed to communicate with remote node.

Solution:

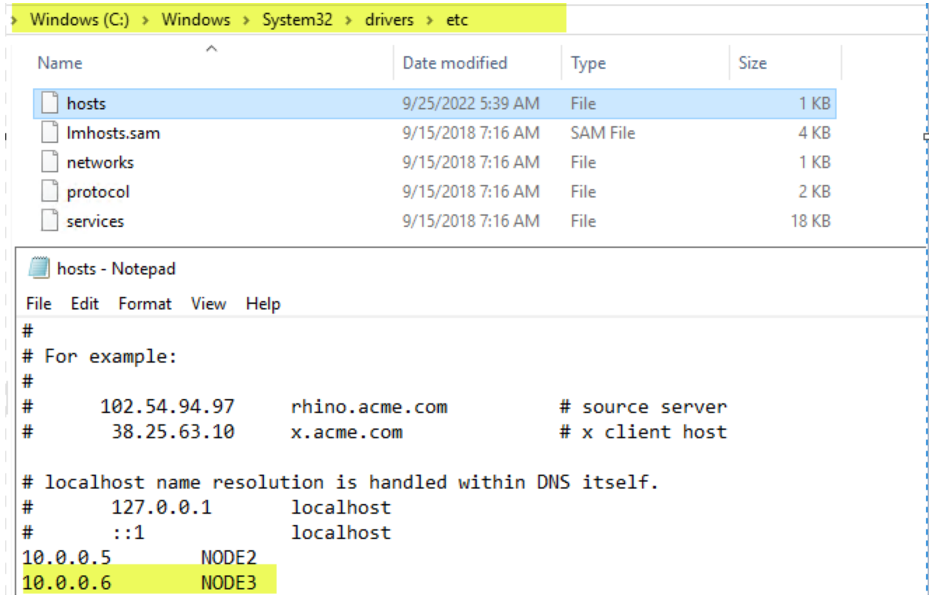
Ensure that the DNS Server is able to resolve the host name to IP address mapping. Alternatively, enter the host name to IP Address mapping in the Windows HOSTS file as a workaround.



No:	Date	Time	Process ID	Thread ID	Log Flag	Component
17336	9/25/2022	5:27:54 AM	8460	8040	Warning	MessageChannel

Message:

Failed to communicate with target node, NODE3. This may be because it is not connected to the same System Management Server as this node (https://node1.rkdc.com). If that is the case, use the Configurator on the target node, NODE3, and point it to the same System Management Server that this node, https://node1.rkdc.com, is pointed to, reboot the target node, NODE3, then try again.


Windows (C:) › Windows › System32 › drivers › etc

Name	Date modified	Type	Size
hosts	9/25/2022 5:39 AM	File	1 KB
lmhosts.sam	9/15/2018 7:16 AM	SAM File	4 KB
networks	9/15/2018 7:16 AM	File	1 KB
protocol	9/15/2018 7:16 AM	File	2 KB
services	9/15/2018 7:16 AM	File	18 KB

```
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
10.0.0.5        NODE2
10.0.0.6        NODE3
```

Troubleshooting

SMS connectivity issue after Hardware Replacement or VM Restoration

Problem:

Following message may be logged in the logger after Hardware Replacement or VM Restoration of a node that was previously connected to SMS.

ArchestrA.CertificateManager: Please un-register the device <device name> from management server. Use the (Remove-AsbDevice) script to remove the device registration

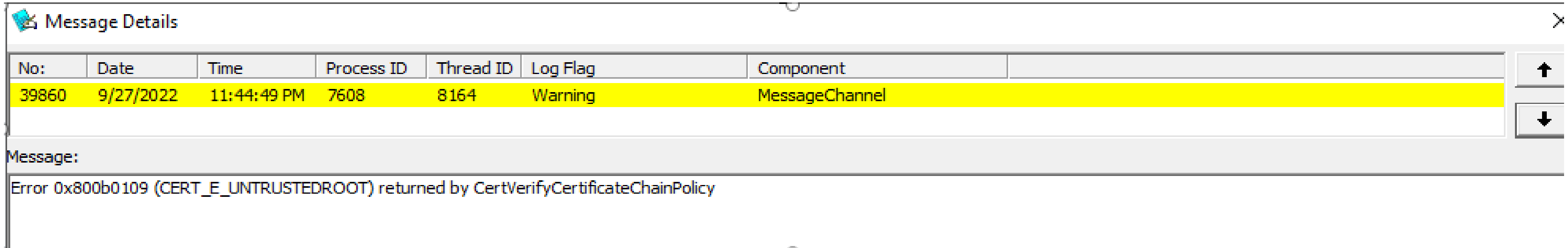
Solution:

Contact AVEVA Global Customer Support (GCS) for the PowerShell script “**Remove-AsbDevice**” and the procedure that needs to be followed to execute the script.

Troubleshooting

Missing certificate on a node configured for SMS

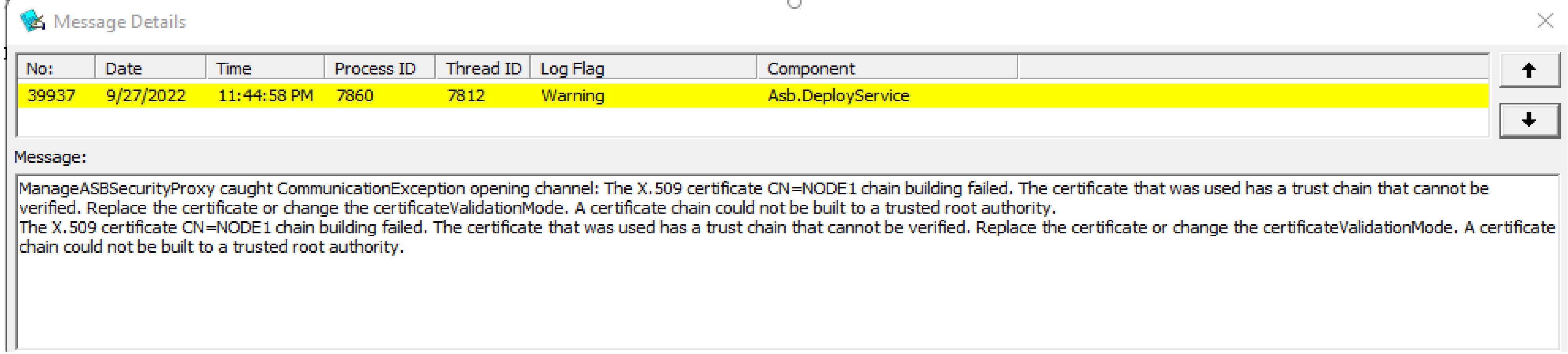
- **Problem**: Below mentioned warnings getting logged in the logger.
- **Solution:** It is most likely due to certificate being missed on a node configured for SMS. Check the certificate in the Certificate Manager (CertMgr.msc). Reconfigure the SMS to install the missing certificate.



No:	Date	Time	Process ID	Thread ID	Log Flag	Component
39860	9/27/2022	11:44:49 PM	7608	8164	Warning	MessageChannel

Message:

Error 0x800b0109 (CERT_E_UNTRUSTEDROOT) returned by CertVerifyCertificateChainPolicy



No:	Date	Time	Process ID	Thread ID	Log Flag	Component
39937	9/27/2022	11:44:58 PM	7860	7812	Warning	Asb.DeployService

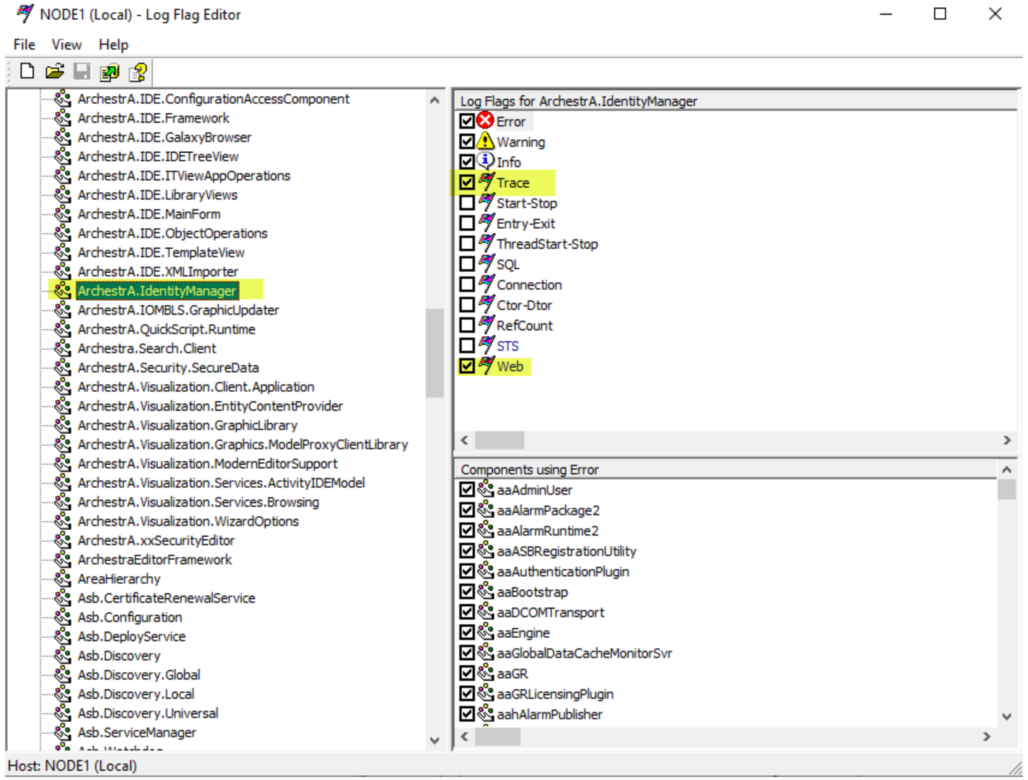
Message:

ManageASBSecurityProxy caught CommunicationException opening channel: The X.509 certificate CN=NODE1 chain building failed. The certificate that was used has a trust chain that cannot be verified. Replace the certificate or change the certificateValidationMode. A certificate chain could not be built to a trusted root authority.
The X.509 certificate CN=NODE1 chain building failed. The certificate that was used has a trust chain that cannot be verified. Replace the certificate or change the certificateValidationMode. A certificate chain could not be built to a trusted root authority.

Troubleshooting

System Management Server configuration

- Capture the Domain or Workgroup details
- Ensure that the logged in user is a member of “Administrators” or “aaAdministrators” groups
- Run the Configurator as “Run As Administrator” option
- Check the drive space in install directory
- Check and export the Root, Intermediate and Personal store certificates for Auto Generated and IT Managed certificates
- Ensure that there is only one ASB generated certificate in each store which has “ASB” tag
- Enable “Trace” and “Web” log flags for these components
  - ArchestrA.IdentityManager
  - ArchestrA.CertificateManager
  - Configurator



ArchestrA.IDE.ConfigurationAccessComponent
ArchestrA.IDE.Framework
ArchestrA.IDE.GalaxyBrowser
ArchestrA.IDE.IDETreeView
ArchestrA.IDE.ITViewAppOperations
ArchestrA.IDE.LibraryViews
ArchestrA.IDE.MainForm
ArchestrA.IDE.ObjectOperations
ArchestrA.IDE.TemplateView
ArchestrA.IDE.XMLImporter
ArchestrA.IdentityManager
ArchestrA.IOMBLS.GraphicUpdater
ArchestrA.QuickScript.Runtime
Archestra.Search.Client
ArchestrA.Security.SecureData
ArchestrA.Visualization.Client.Application
ArchestrA.Visualization.EntityContentProvider
ArchestrA.Visualization.GraphicLibrary
ArchestrA.Visualization.Graphics.ModelProxyClientLibrary
ArchestrA.Visualization.ModernEditorSupport
ArchestrA.Visualization.Services.ActivityIDEModel
ArchestrA.Visualization.Services.Browsing
ArchestrA.Visualization.WizardOptions
ArchestrA.xxSecurityEditor
ArchestraEditorFramework
AreaHierarchy
Asb.CertificateRenewalService
Asb.Configuration
Asb.DeployService
Asb.Discovery
Asb.Discovery.Global
Asb.Discovery.Local
Asb.Discovery.Universal
Asb.ServiceManager

Log Flags for ArchestrA.IdentityManager

☑ Error
☑ Warning
☑ Info
☑ Trace
☐ Start-Stop
☐ Entry-Exit
☐ ThreadStart-Stop
☐ SQL
☐ Connection
☐ Ctor-Dtor
☐ RefCount
☐ STS
☑ Web

Components using Error

☑ aaAdminUser
☑ aaAlarmPackage2
☑ aaAlarmRuntime2
☑ aaASBRegistrationUtility
☑ aaAuthenticationPlugin
☑ aaBootstrap
☑ aaDCOMTransport
☑ aaEngine
☑ aaGlobalDataCacheMonitorSvr
☑ aaGR
☑ aaGRLicensingPlugin
☑ aahAlarmPublisher

Host: NODE1 (Local)

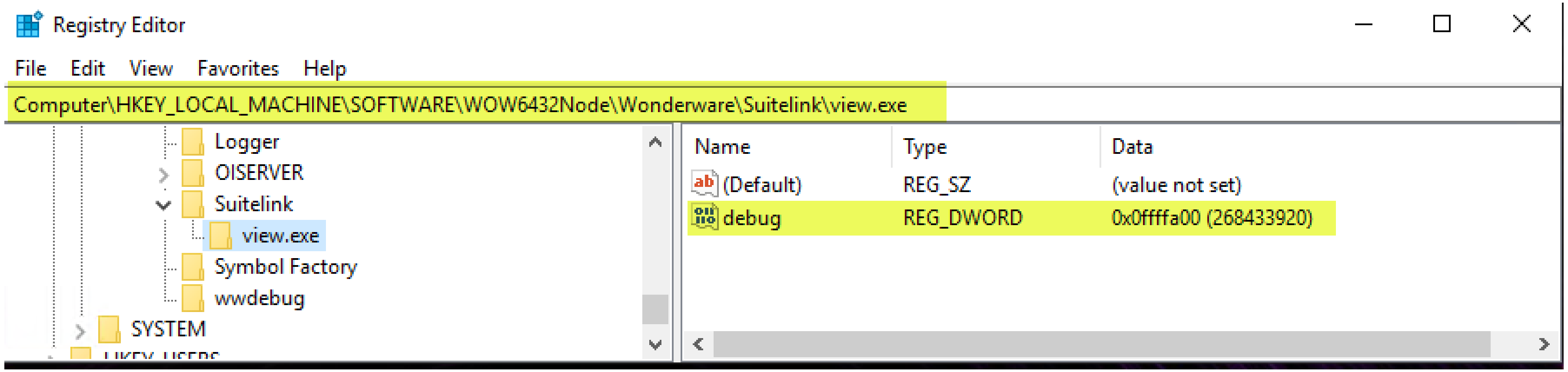
Troubleshooting

Secured Communication

- Secured Suitelink Communication

  Enter a DWORD value named “debug” with the Hexadecimal value 0X0FFFFA00 under the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Wonderware\Suitelink\<ProcessName>**

- Analyze the log messages in the SMC Logger from WWSLS component



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Wonderware\Suitelink\view.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
debug	REG_DWORD	0x0ffffa00 (268433920)

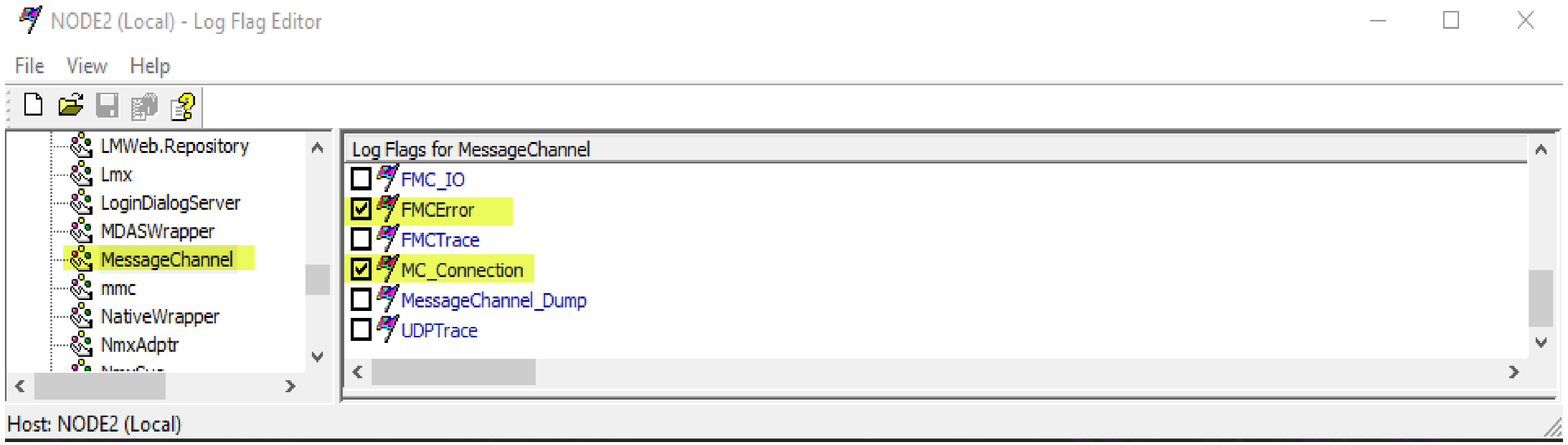
Troubleshooting

Secured Communication …cont’d

- Secured MX Communication

  Enable log flags “**FMCError**” and “**MC_Connection**” for the “**MessageChannel**” component in the OCMC

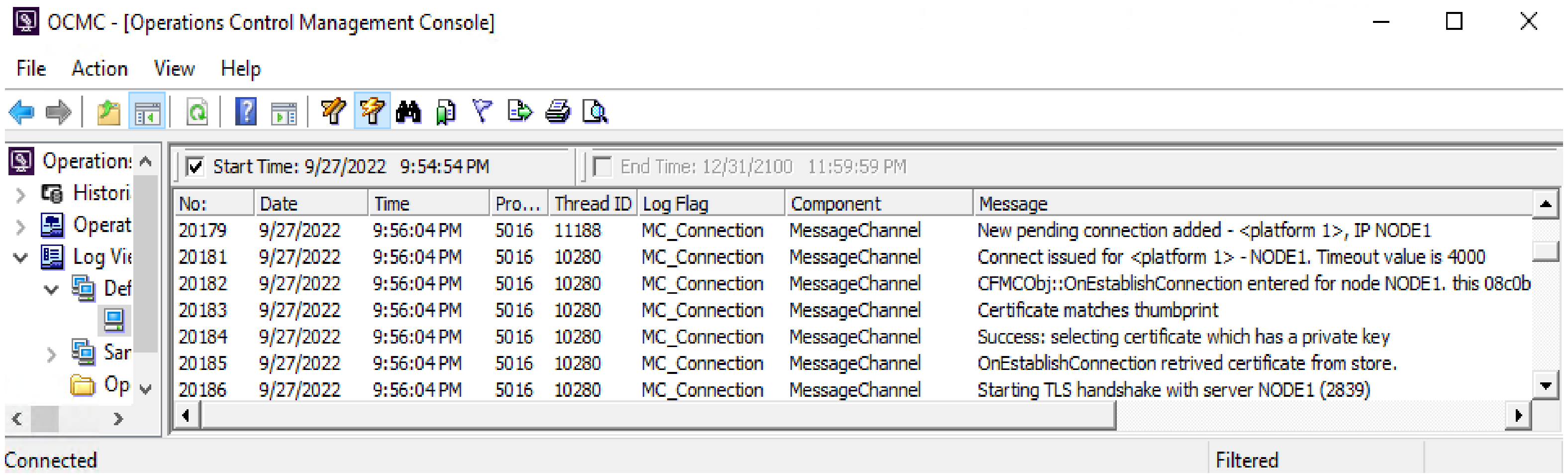
- Analyze the log messages in the OCMC Logger



Log Flags for MessageChannel

- □ FMC_IO
- ☑ FMCError
- □ FMCTrace
- ☑ MC_Connection
- □ MessageChannel_Dump
- □ UDPTrace

Host: NODE2 (Local)



☑ Start Time: 9/27/2022 9:54:54 PM □ End Time: 12/31/2100 11:59:59 PM

No:	Date	Time	Pro...	Thread ID	Log Flag	Component	Message
20179	9/27/2022	9:56:04 PM	5016	11188	MC_Connection	MessageChannel	New pending connection added - <platform 1>, IP NODE1
20181	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	Connect issued for <platform 1> - NODE1. Timeout value is 4000
20182	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	CFMCObj::OnEstablishConnection entered for node NODE1. this 08c0b
20183	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	Certificate matches thumbprint
20184	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	Success: selecting certificate which has a private key
20185	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	OnEstablishConnection retrived certificate from store.
20186	9/27/2022	9:56:04 PM	5016	10280	MC_Connection	MessageChannel	Starting TLS handshake with server NODE1 (2839)

Connected Filtered

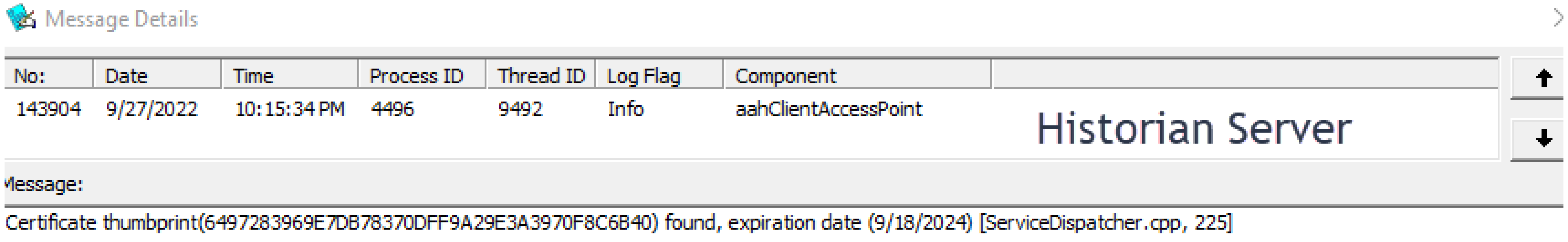
Troubleshooting

Secured Communication …cont’d

- Secured HCAL-HCAP Communication

  Enable log flags “**aahClientAccessPoint**” component on server and “**aahClientCommon**” component on the client

- Analyze the log messages in the SMC Logger

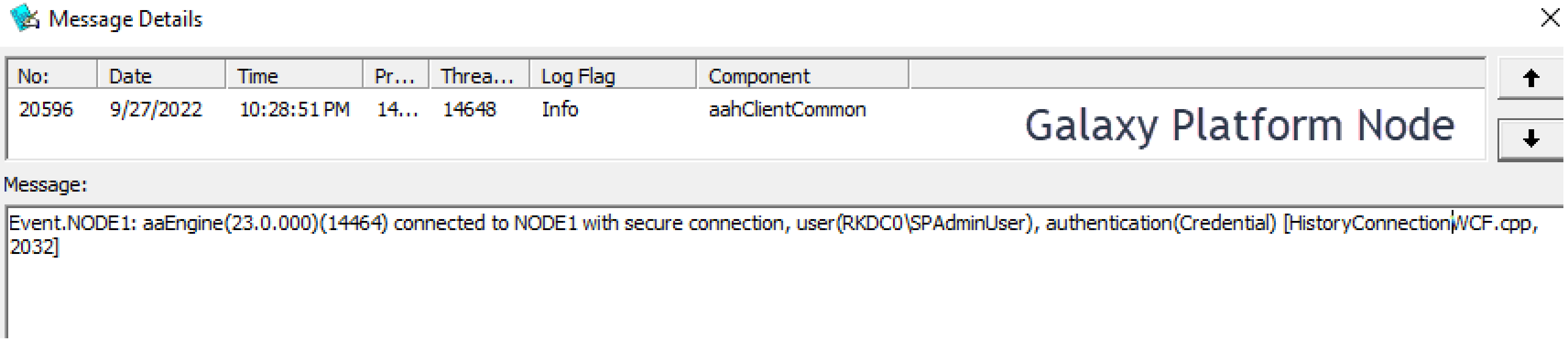


No:	Date	Time	Process ID	Thread ID	Log Flag	Component
143904	9/27/2022	10:15:34 PM	4496	9492	Info	aahClientAccessPoint

Historian Server

Message:

```
Certificate thumbprint(6497283969E7DB78370DFF9A29E3A3970F8C6B40) found, expiration date (9/18/2024) [ServiceDispatcher.cpp, 225]
```



No:	Date	Time	Pr…	Threa…	Log Flag	Component
20596	9/27/2022	10:28:51 PM	14…	14648	Info	aahClientCommon

Galaxy Platform Node

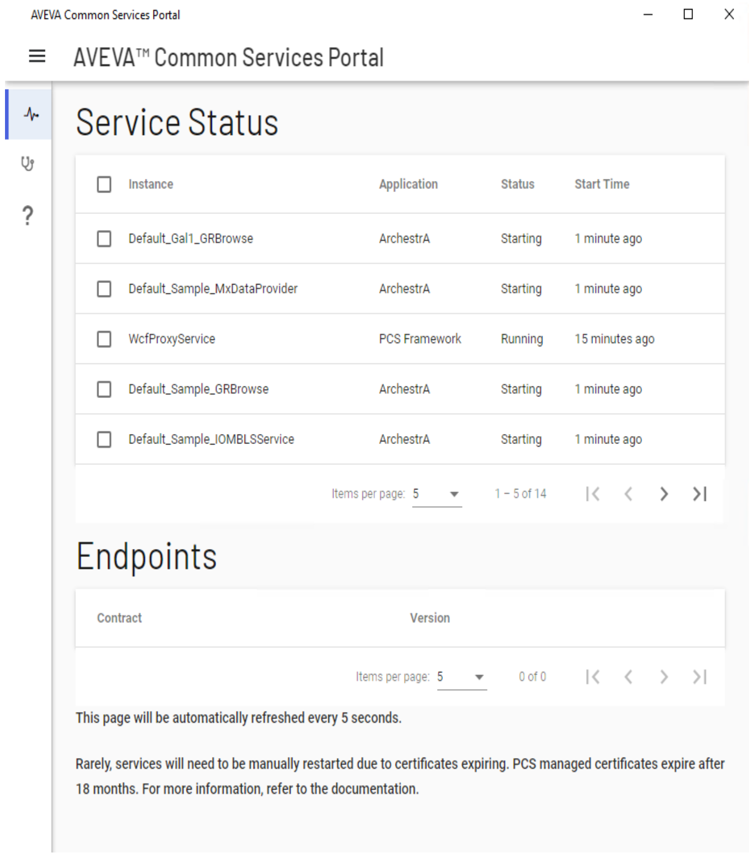
Message:

```
Event.NODE1: aaEngine(23.0.000)(14464) connected to NODE1 with secure connection, user(RKDC0\SPAdminUser), authentication(Credential) [HistoryConnectionWCF.cpp,
2032]
```

Troubleshooting

Platform Common Services

- Launch the “Common Services Portal” from the Windows Start Menu
- Open the Service Status page and check the status of services
- Open the Troubleshooting page and press the SCAN button to run the diagnostics



Service Status

□	Instance	Application	Status	Start Time
□	Default_Gal1_GRBrowse	ArchestrA	Starting	1 minute ago
□	Default_Sample_MxDataProvider	ArchestrA	Starting	1 minute ago
□	WcfProxyService	PCS Framework	Running	15 minutes ago
□	Default_Sample_GRBrowse	ArchestrA	Starting	1 minute ago
□	Default_Sample_IOMBLSService	ArchestrA	Starting	1 minute ago

Items per page: 5   1 – 5 of 14

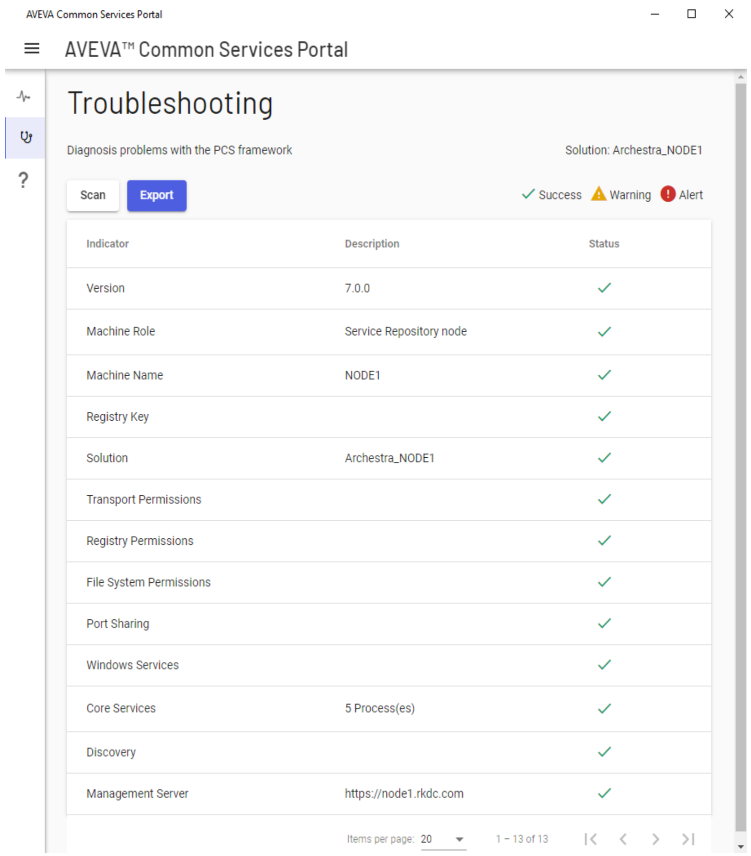
Endpoints

Contract	Version

Items per page: 5   0 of 0

This page will be automatically refreshed every 5 seconds.

Rarely, services will need to be manually restarted due to certificates expiring. PCS managed certificates expire after 18 months. For more information, refer to the documentation.



Troubleshooting

Diagnosis problems with the PCS framework

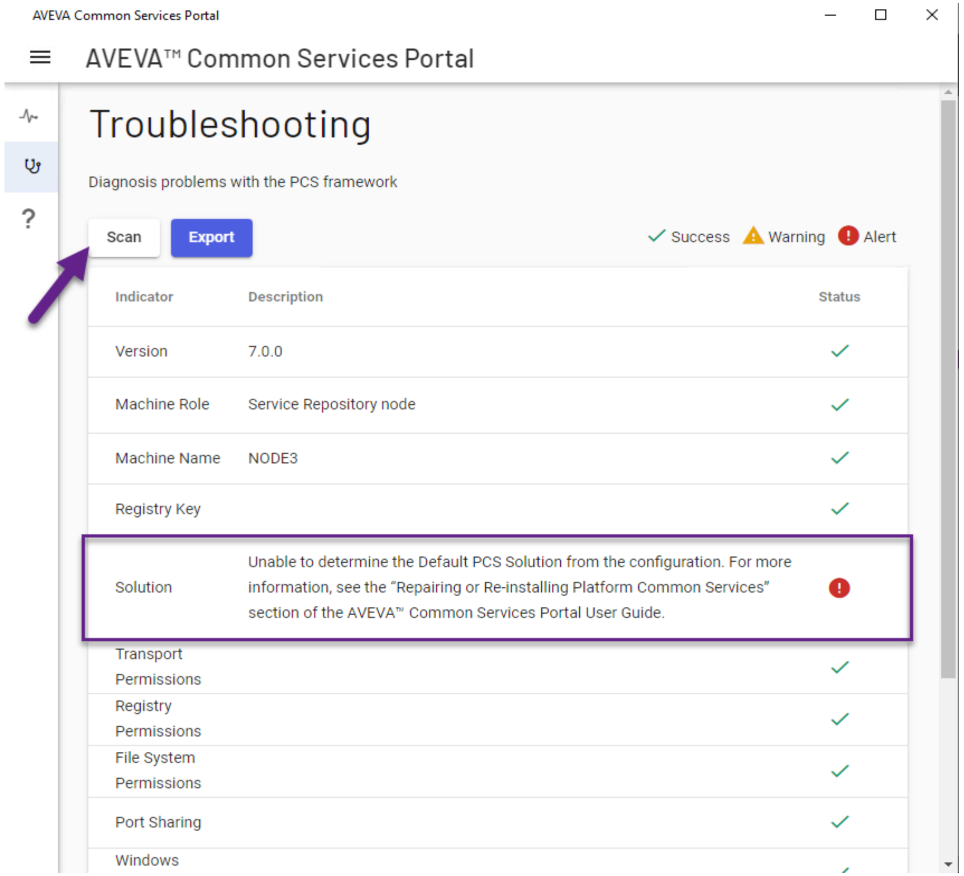
Solution: Archestra_NODE1

Indicator	Description	Status
Version	7.0.0	✓
Machine Role	Service Repository node	✓
Machine Name	NODE1	✓
Registry Key		✓
Solution	Archestra_NODE1	✓
Transport Permissions		✓
Registry Permissions		✓
File System Permissions		✓
Port Sharing		✓
Windows Services		✓
Core Services	5 Process(es)	✓
Discovery		✓
Management Server	https://node1.rkdc.com	✓

Items per page: 20   1 – 13 of 13

Troubleshooting

Platform Common Services Issue – An Example



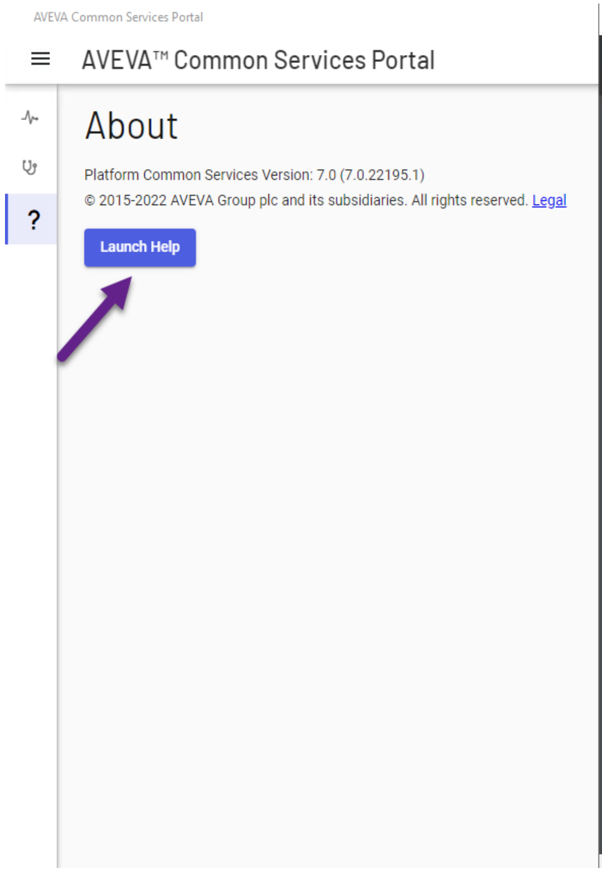
AVEVA Common Services Portal
AVEVA™ Common Services Portal

Troubleshooting

Diagnosis problems with the PCS framework

Scan
Export
✓ Success ⚠ Warning ❗ Alert

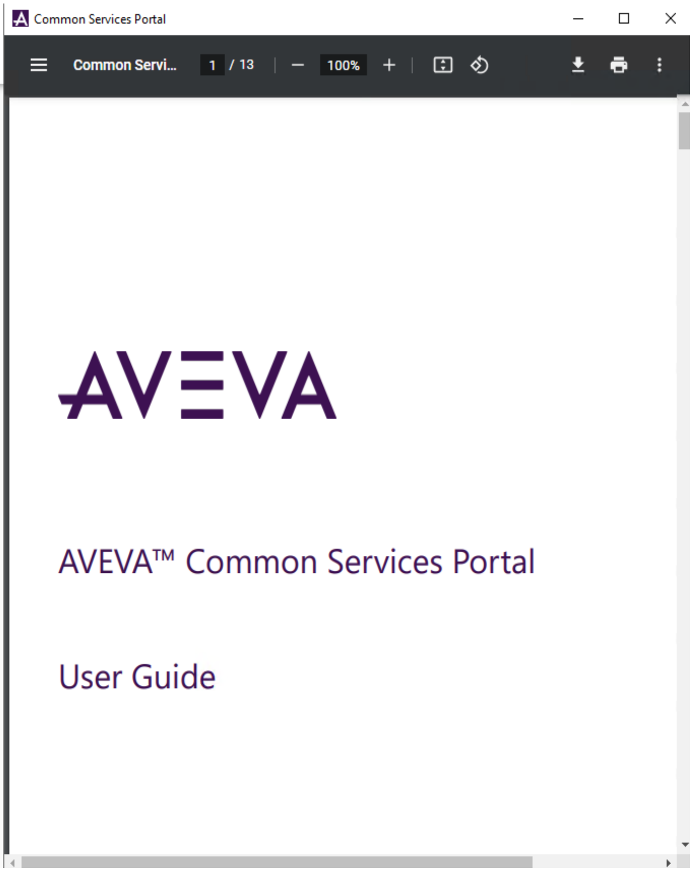
Indicator	Description	Status
Version	7.0.0	✓
Machine Role	Service Repository node	✓
Machine Name	NODE3	✓
Registry Key		✓
Solution	Unable to determine the Default PCS Solution from the configuration. For more information, see the "Repairing or Re-installing Platform Common Services" section of the AVEVA™ Common Services Portal User Guide.	❗
Transport Permissions		✓
Registry Permissions		✓
File System Permissions		✓
Port Sharing		✓
Windows		



About

Platform Common Services Version: 7.0 (7.0.22195.1)

© 2015-2022 AVEVA Group plc and its subsidiaries. All rights reserved. Legal



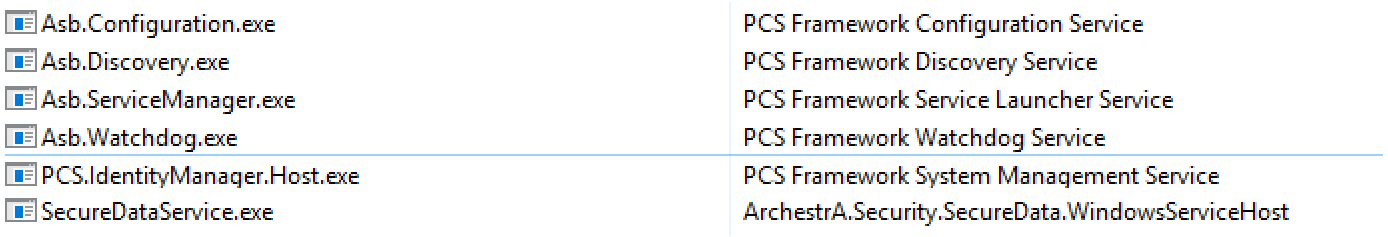
AVEVA™ Common Services Portal

User Guide

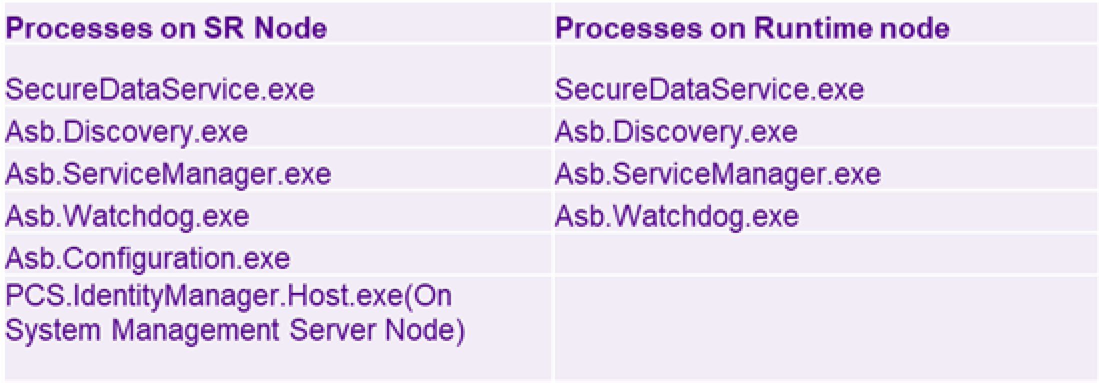
Troubleshooting

Platform Common Services…cont’d

- Ensure that Net.TCP Port Sharing service is running
- Ensure that PCS services and associated processes are running



Asb.Configuration.exe	PCS Framework Configuration Service
Asb.Discovery.exe	PCS Framework Discovery Service
Asb.ServiceManager.exe	PCS Framework Service Launcher Service
Asb.Watchdog.exe	PCS Framework Watchdog Service
PCS.IdentityManager.Host.exe	PCS Framework System Management Service
SecureDataService.exe	ArchestrA.Security.SecureData.WindowsServiceHost



Processes on SR Node	Processes on Runtime node
SecureDataService.exe	SecureDataService.exe
Asb.Discovery.exe	Asb.Discovery.exe
Asb.ServiceManager.exe	Asb.ServiceManager.exe
Asb.Watchdog.exe	Asb.Watchdog.exe
Asb.Configuration.exe	
PCS.IdentityManager.Host.exe(On System Management Server Node)	

Troubleshooting

Platform Common Services…cont’d

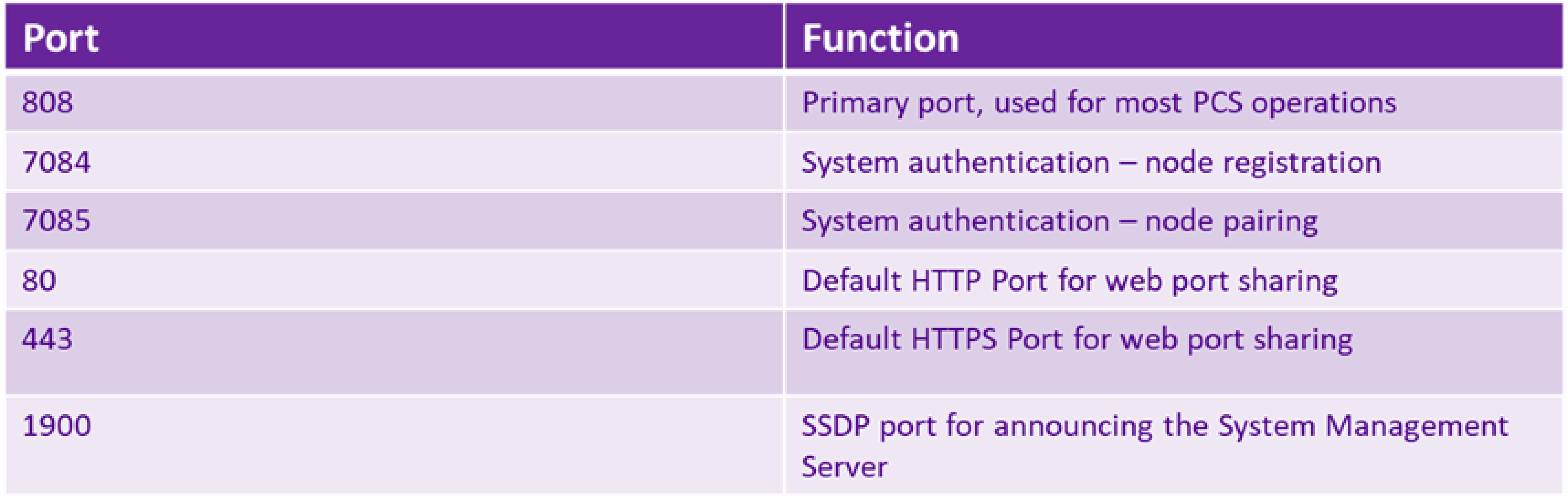
- Ensure that the following virtual accounts are present and belong to the corresponding Windows Groups

	PCS User Groups	Virtual accounts	Account Permissions
1	ASBCoreServices	NT SERVICE\Watchdog_Service NT SERVICE\AIMTokenHost	Full Control permissions on most files and registry keys
2	ASBSolution	NT SERVICE\Watchdog_Service NT SERVICE\AsbServiceManager	Read & Execute permissions on all files and registry keys
3	ArchestrAWebHosting	NT SERVICE\Watchdog_Service NT SERVICE\AsbServiceManager NT SERVICE\AIMTokenHost	Permission to reserve HTTP URLs, Private key of binding certificates.

Troubleshooting

Platform Common Services…cont'd

- Ensure that the following ports are opened in the Firewall



Port	Function
808	Primary port, used for most PCS operations
7084	System authentication – node registration
7085	System authentication – node pairing
80	Default HTTP Port for web port sharing
443	Default HTTPS Port for web port sharing
1900	SSDP port for announcing the System Management Server

Raghu Kanchanapally

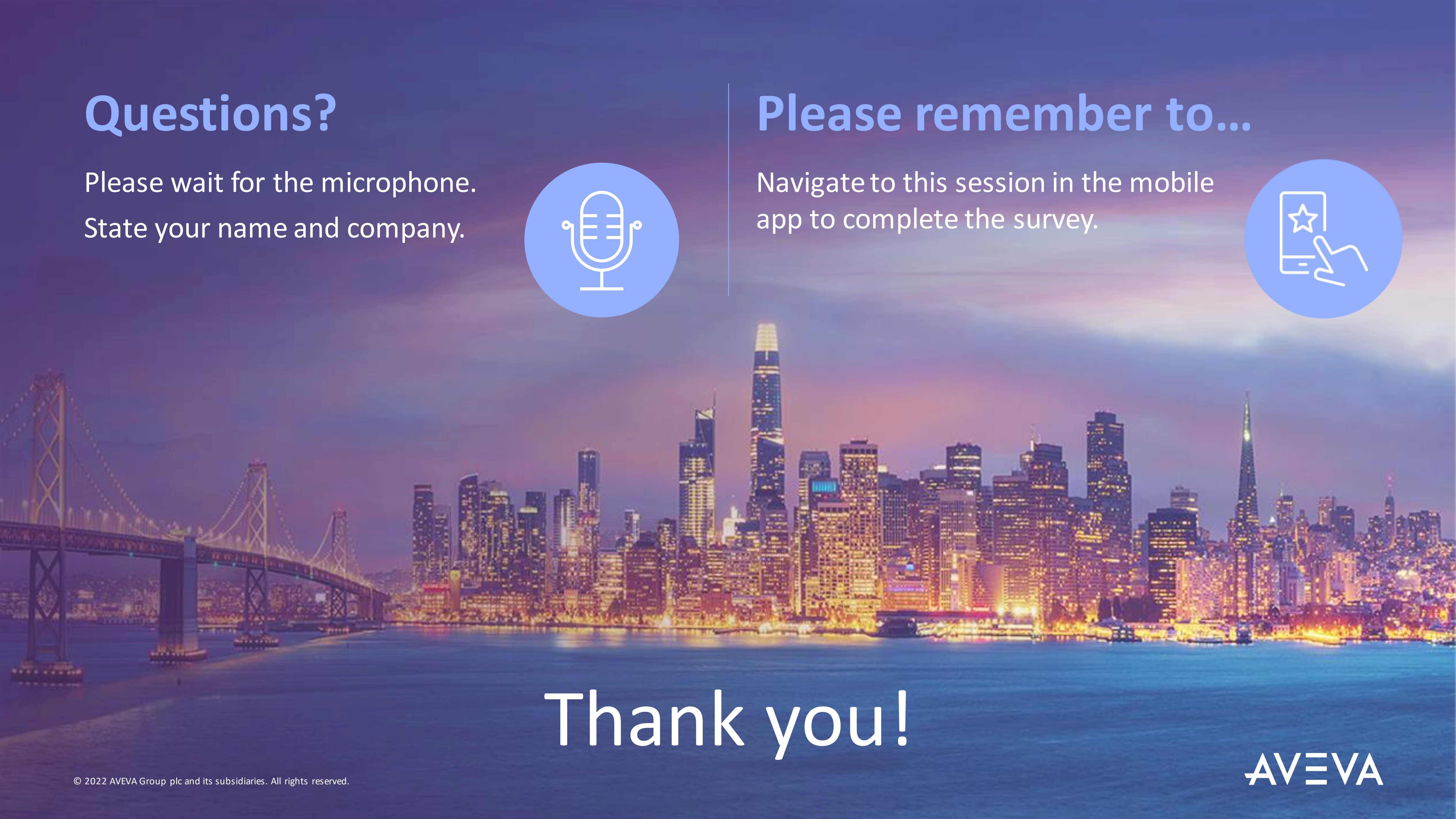
Principal Technical Account Manager

- AVEVA
- Raghu.Kanchanapally@aveva.com

Jerry Lau

Senior Manager

- AVEVA
- Jerry.Lau@aveva.com



Questions?

Please wait for the microphone.

State your name and company.

Please remember to…

Navigate to this session in the mobile app to complete the survey.

Thank you!

AVEVA

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

AVEVA

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a global leader in industrial software, sparking ingenuity to drive responsible use of the world's resources. The company's secure industrial cloud platform and applications enable businesses to harness the power of their information and improve collaboration with customers, suppliers and partners.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. With operations around the globe, we are headquartered in Cambridge, UK and listed on the London Stock Exchange's FTSE 100.

Learn more at www.aveva.com

AVEVA