UNISYS | Securing Your Tomorrow®

New Security Features in AB Suite

Andy Wardle | Senior Architect
Gary Taylor | Senior Architect

Security – Why Bother?

- In 2020 the global average cost of a data breach amounted to US$3.86 million
- Organisations have a need to safeguard and protect their sensitive data
- Organisations often have regulatory and/or audit requirements to encrypt sensitive data in databases
- Organisations are increasingly concerned about security breaches adversely impacting their reputation and finances
- Personally Identifiable Information (PII), financial data, and other sensitive details communicated between client and server components need to be secured
- The EU GDPR regulations have formalised many of these requirements
  - And they have spawned similar regulations around the world

Security is in the Unisys DNA

ur

Information Technology Laboratory

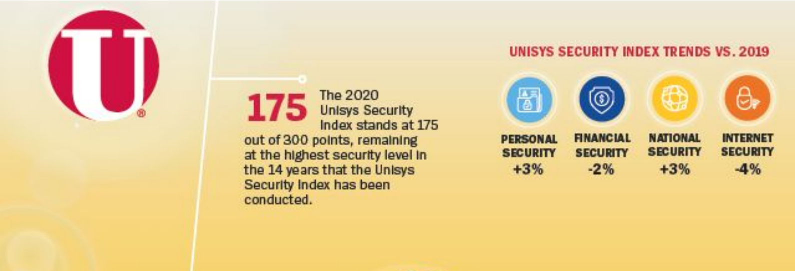
NATIONAL V

Institute of
s and Technology
tment of Commerce

Operati	Data
Unisys ClearF	
Unisys ClearF	
IBM System z	
OpenVMS	
IBM System i	
HP-UX	
IBM AIX	
Unix	
Solaris	
Linux	8,381
Windows	9,675

Data Taken 8/13/21

This chart was developed by Unisys and represents Unisys' interpretation of publicly available NIST



UNISYS SECURITY INDEX TRENDS VS. 2019

175 The 2020 Unisys Security Index stands at 175 out of 300 points, remaining at the highest security level in the 14 years that the Unisys Security Index has been conducted.

PERSONAL SECURITY	FINANCIAL SECURITY	NATIONAL SECURITY	INTERNET SECURITY
+3%	-2%	+3%	-4%

2020 Unisys Security Index™

CONSUMERS' SECURITY CONCERNS GLOBALLY

Global Edition

UNISYS | Securing Your Tomorrow®

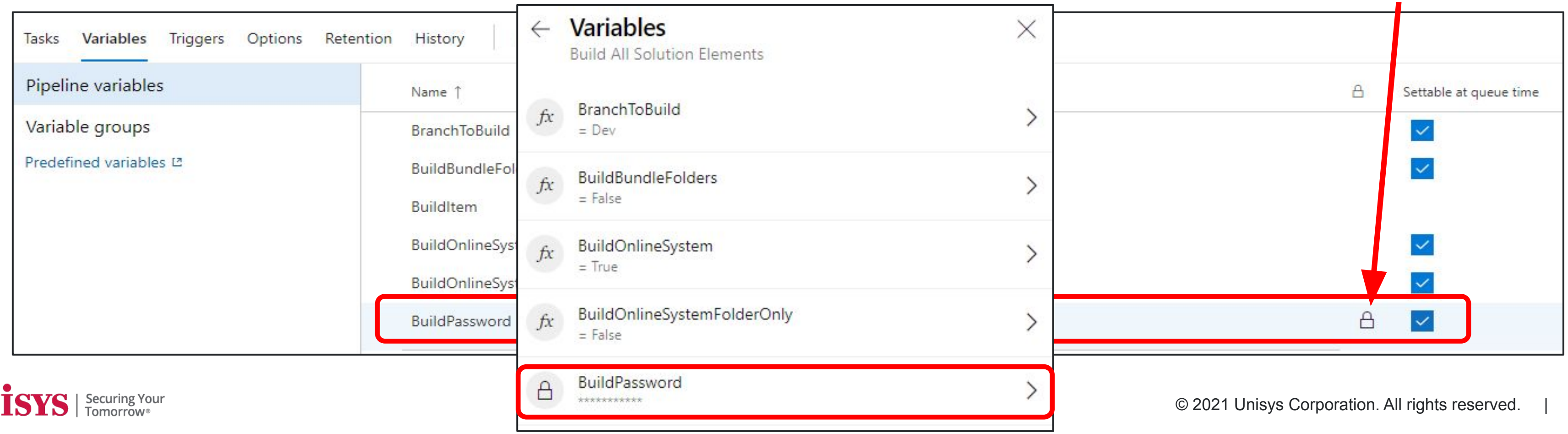
unisyssecurityindex.com
#SecurityIndex

Common Features

Secure Passwords in Build Automation

- Azure DevOps Pipelines (previously TFS Build Definitions)
  - This is a feature of Azure DevOps (previously TFS), not AB Suite per se
  - Build automation with TFS/Azure DevOps has been supported since AB Suite 5.0
  - Define the password as a Pipeline Variable
  - Click on the Padlock to encrypt the password

Click to Encrypt the Password



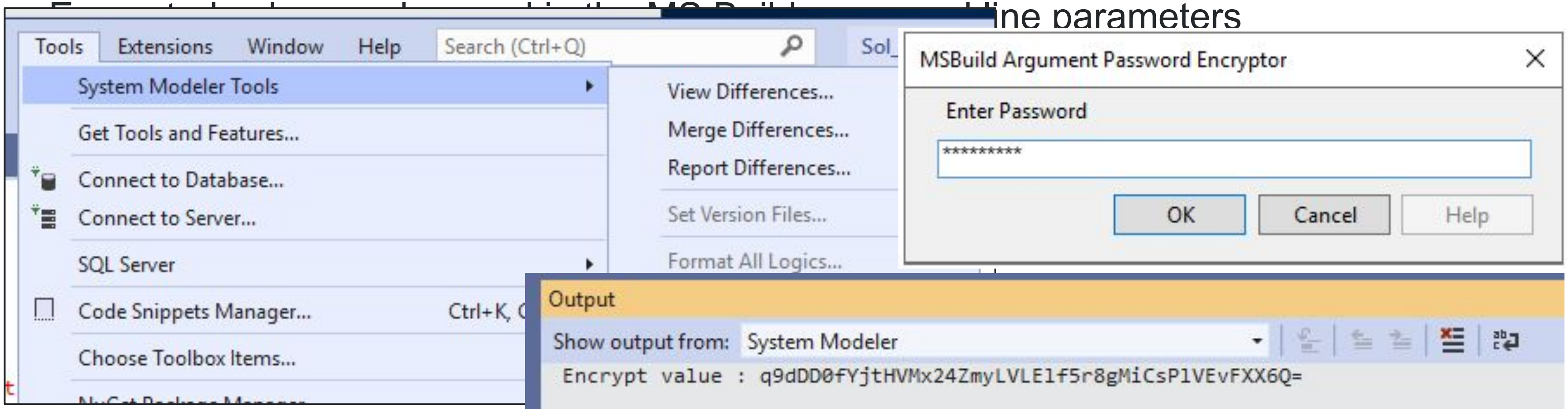
Name ↑	🔒	Settable at queue time
BranchToBuild		☑
BuildBundleFol		☑
BuildItem		
BuildOnlineSys		☑
BuildOnlineSys		☑
BuildPassword	🔒	☑

Variables
Build All Solution Elements

- BranchToBuild = Dev
- BuildBundleFolders = False
- BuildOnlineSystem = True
- BuildOnlineSystemFolderOnly = False
- 🔒 BuildPassword ***********

Secure Passwords in Build Automation

- MS Build Password Encryption
  - New in AB Suite 8.0
  - Previously passwords provided for command line builds had to be included in plain text
  - Developer now provides menu options to encrypt a password
  - Encrypted value can be used in the MS Build command line parameters



Enter Password: *********

Show output from: System Modeler

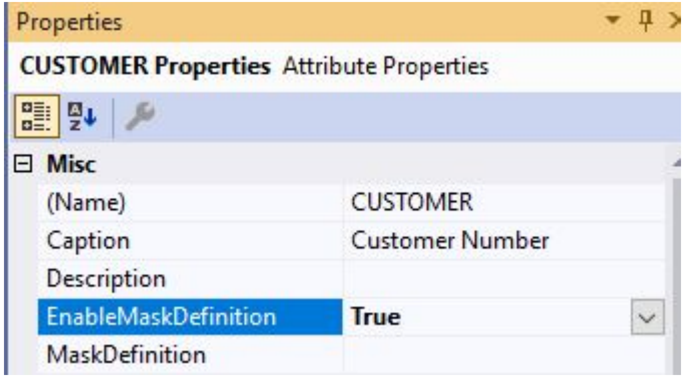
```
Encrypt value : q9dDD0fYjtHVMx24ZmyLVLE1f5r8gMiCsP1VEvFXX6Q=
```

Component Enabler Support for TLS 1.2

- Protects Data in Motion
- Capability first introduced in 7.0 for MCP
  - Other platforms are part of 8.0 release
  - TLS 1.3 not supported
- Implementation via a simple configuration change
  - Change Connection URI
    - Non TLS `x-ratl:<hostname>:<port>` e.g. `x-ratl:GBMKMCP:2910`
    - TLS `x-ratltls:<hostname>:<port>` e.g. `x-ratltls:GBMKMCP:2910`
- All other changes handled by latest Component Enabler APIs
  - Just rebuild existing clients referencing 8.0 CE APIs
  - Change configuration
  - Configure at host – Covered later

Log Masking

- Provides ability to mask fields in “LINC” Logs/Audit Logs
- By default “LINC” Logs/Audit Logs store all message text in plain text
- Enabling Masking for a field will write asterisks (*) to the log for that field rather than real data
  - Specifying a Mask Definition allows you to specify an alternative character to the asterisk
  - Actual data is never recorded
- Both options are Attribute Properties



CUSTOMER Properties Attribute Properties

Misc

(Name)	CUSTOMER
Caption	Customer Number
Description	
EnableMaskDefinition	**True**
MaskDefinition	

UNISYS | Securing Your Tomorrow®

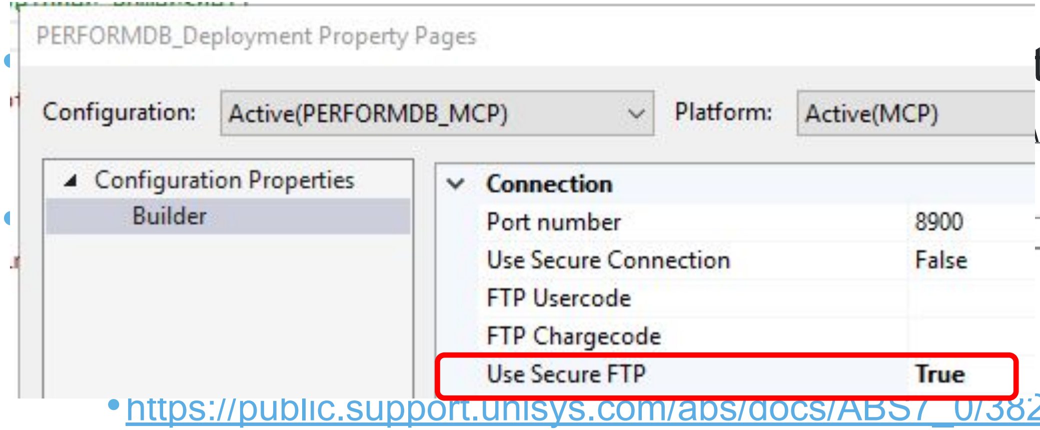
MCP Runtime Features

Secure FTP for Builds

- AB Suite 7.0 IC 1018 onwards
- Adds option to use FTPS when transferring generated source code to MCP
  - Many clients currently require security waivers to use non-secure FTP
- Requires MCP TCP/IP SSL to be active
  - NW TCPIP OPT +SSL
- Requires specific MCP FTP Server configuration settings …
  - AUTHMODE = SSL
  - SSLMODE = IMPLICIT
  - SSL_SERVICENAME = “FTPTLS” (this is the Certificate Name defined in Security Centre)
  - INITIATE_SSL_SERVER = 1
  - Modify SYSTEM/FTP/SUPPORT/CONFIGURATION to make these permanent

Secure FTP for Builds

- Also requires Developer configuration changes
- In 8.0 set the Deployment Folder Configuration “Use Secure FTP” option to True



PERFORMDB_Deployment Property Pages

Configuration: Active(PERFORMDB_MCP) Platform: Active(MCP)

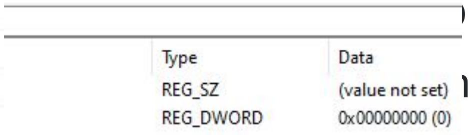
Configuration Properties
- Builder

Connection	
Port number	8900
Use Secure Connection	False
FTP Usercode	
FTP Chargecode	
Use Secure FTP	True

tting named “SecureFTP”

\Unisys\System Modeler\Features\Builder

uild server



Type	Data
REG_SZ	(value not set)
REG_DWORD	0x00000000 (0)

n and

- https://public.support.unisys.com/abs/docs/ABS7_0/38265815-009.pdf

Secure non-FTP Connections for Builds

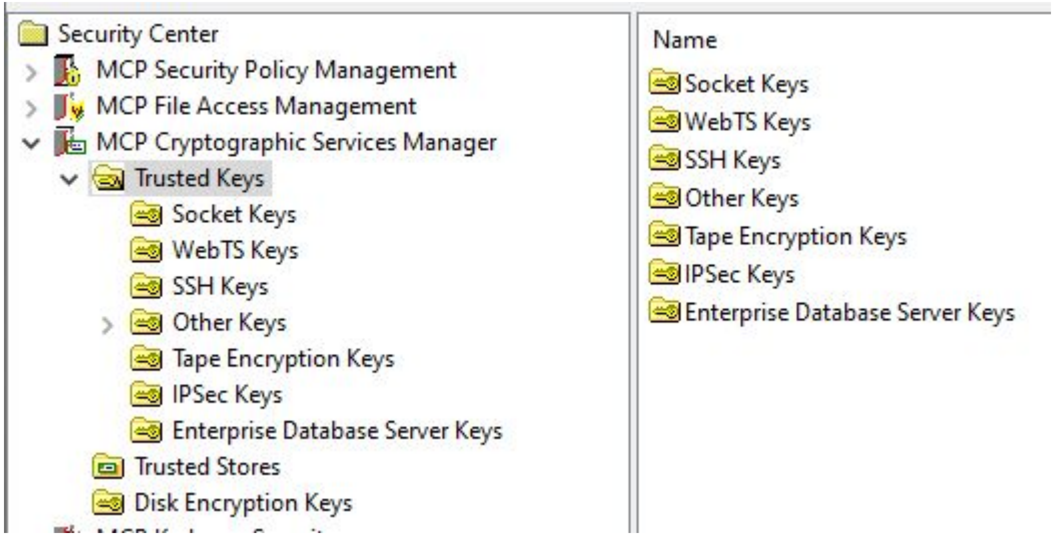
- New in AB Suite 8.0
- Uses FTP over TLS 1.2
- Encrypts all communications between the Windows Builder Client to the MCP Application Builder server (APPL_BLD)
  - Meaning all build-related communications can now be secured
  - Including MCP passwords
- Requires a TLS certificate to be configured for FTP on MCP
  - Must also be installed in the Windows Trusted Store
- Uses implicit secure FTP port 990

Secure RATL

- Protects Data in Motion
- AB Suite 7.0 onwards
- Only supports TLS 1.2
- Requires MCP CryptoAPI services and TCP/IP SSL to be active
  - NA MCAPI {+/-/STATUS}
  - NW TCPIP OPT +SSL
- MCP changes required …
  - New cryptographic key defined in Security Center
  - New RATL definitions in CCF parameter file
- Requires access to a Certificate Authority to authorise cryptographic key

Secure RATL – Cryptographic Key in Security Center

- Start Security Center
- Select MCP Cryptographic Services Manager
- Specify MCP Host
- Select Trusted Keys



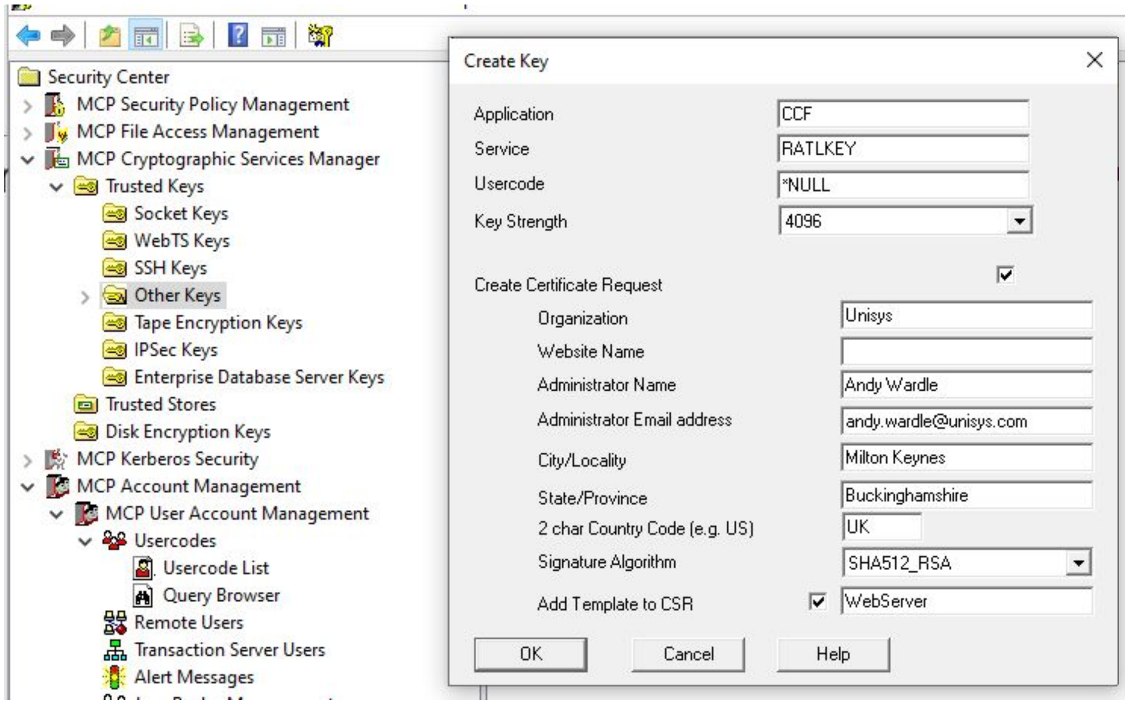
- Security Center
  - MCP Security Policy Management
  - MCP File Access Management
  - MCP Cryptographic Services Manager
    - Trusted Keys
      - Socket Keys
      - WebTS Keys
      - SSH Keys
      - Other Keys
      - Tape Encryption Keys
      - IPSec Keys
      - Enterprise Database Server Keys
    - Trusted Stores
    - Disk Encryption Keys

Name

- Socket Keys
- WebTS Keys
- SSH Keys
- Other Keys
- Tape Encryption Keys
- IPSec Keys
- Enterprise Database Server Keys

Secure RATL – Request Crypto Key in Security Center

- Right click on Other Keys and select Create Key
- Set Application, e.g. CCF
- Set Service Name, e.g. RATLKEY
- Set Usercode to *NULL
- Set Key Strength to >= 2048
- Check "Create Certificate Request"
- Set Signature Algorithm
- Click on OK, then Save file



Security Center
- MCP Security Policy Management
- MCP File Access Management
- MCP Cryptographic Services Manager
  - Trusted Keys
    - Socket Keys
    - WebTS Keys
    - SSH Keys
    - Other Keys
    - Tape Encryption Keys
    - IPSec Keys
    - Enterprise Database Server Keys
  - Trusted Stores
  - Disk Encryption Keys
- MCP Kerberos Security
- MCP Account Management
  - MCP User Account Management
    - Usercodes
      - Usercode List
      - Query Browser
    - Remote Users
    - Transaction Server Users
    - Alert Messages

Create Key

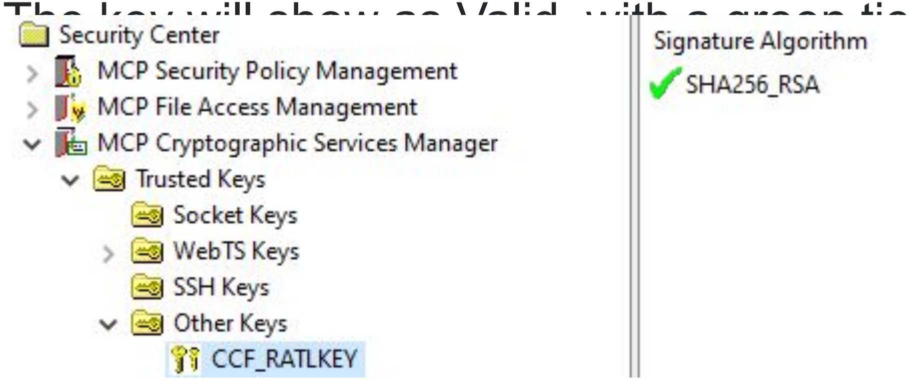
Application	CCF
Service	RATLKEY
Usercode	*NULL
Key Strength	4096
Create Certificate Request	☑
Organization	Unisys
Website Name	
Administrator Name	Andy Wardle
Administrator Email address	andy.wardle@unisys.com
City/Locality	Milton Keynes
State/Province	Buckinghamshire
2 char Country Code (e.g. US)	UK
Signature Algorithm	SHA512_RSA
Add Template to CSR ☑	WebServer

Secure RATL – Authorise Crypto Key

- The key request (.req) file created in Security Center must be authorised by a Certificate Authority
- This will provide a .P7B or .P7C certificate file that must be imported into MCP

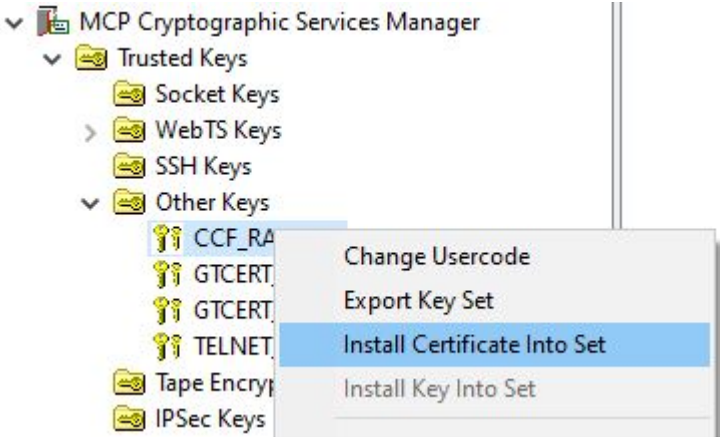
Secure RATL – Import Certificate in Security Center

- Expand Key Store
- Right click on RATL key
- Select Install Certificate into Set
- In browser select .P7B or .P7C and choose
- The key will show as Valid, with a green tic


Security Center
MCP Security Policy Management
MCP File Access Management
MCP Cryptographic Services Manager
Trusted Keys
Socket Keys
WebTS Keys
SSH Keys
Other Keys
CCF_RATLKEY

Signature Algorithm

✓ SHA256_RSA



Secure RATL – Add Definitions to CCF Parameter File

- Add new Service

NAME	As desired, e.g. RATLSSL

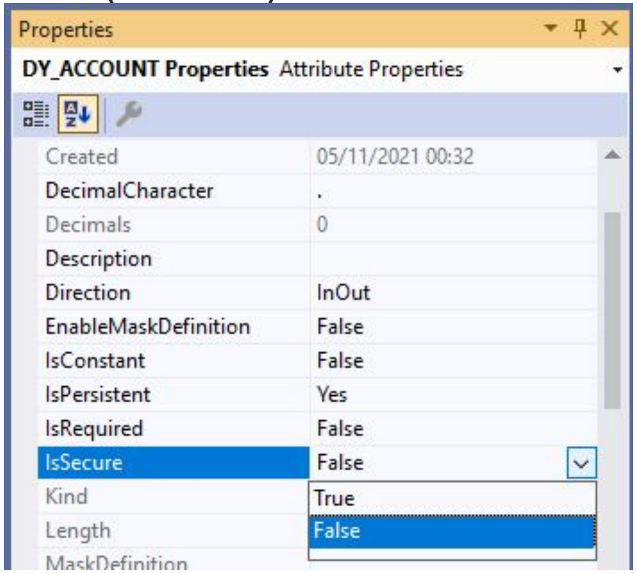
- Add new Port

NAME	As desired, e.g. RATLSSL
SERVICE	Same as new Service, e.g. RATLSSL
SOCKET	As desired, e.g. 2009
SSLSECUREMODE	TRUE
SSLKEYCONTAINER	As defined in Security Center, e.g. CCF_RATLKEY

- See NGEN28/SAMPLE/CCF/PARAMS/RATL for full details

Support for DMS II Encryption

- Offers Data at Rest protection for user data
- Structure Level Encryption (SLE) is supported in AB Suite 8.0
  - Encrypts a complete Ispec (data set) and all associated Profiles (indexes)
  - Easy to configure
  - Set the SecureTechnique property of Ispec class to “StructureEncryption”
- Field Level Encryption (FLE) supported in AB Suite 7.0
  - Encrypts specific Persistent attributes with an Ispec class
  - Set the “IsSecure” attribute property to “True”
    - A Segment property defines the encryption that’s applied
  - Cannot be used for Ordinates, or attributes used in Profile conditions



Properties

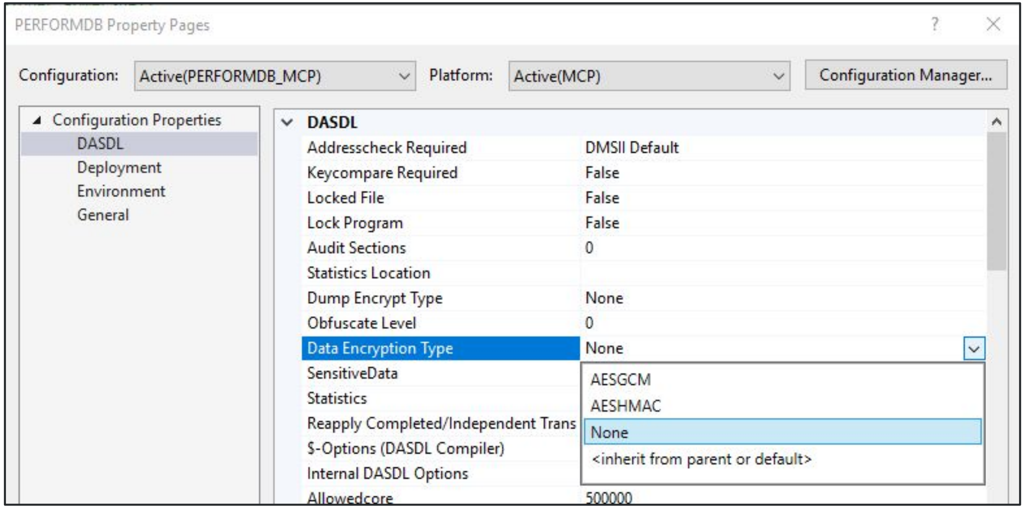
DY_ACCOUNT Properties Attribute Properties

Created	05/11/2021 00:32
DecimalCharacter	.
Decimals	0
Description	
Direction	InOut
EnableMaskDefinition	False
IsConstant	False
IsPersistent	Yes
IsRequired	False
IsSecure	False
Kind	
Length	
MaskDefinition	

True
False

Support for DMS II Encryption

- Encryption is enabled, and algorithm selected, in the Segment Configuration property “Data Encryption Type”
- Algorithm choices are
  - AESGCM
  - AESHMAC (Only supported for Field Level Encryption)
- Only takes effect once an Ispec class or a persistent attribute have their SecureTechnique property enabled



PERFORMDB Property Pages

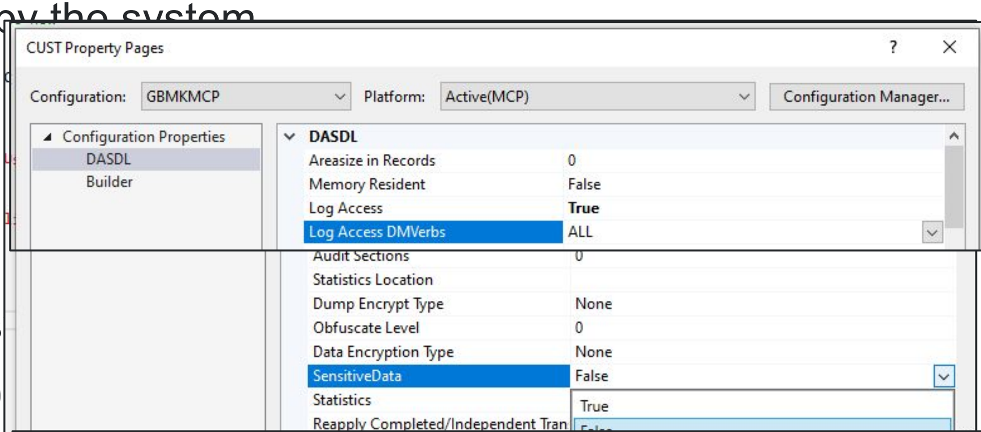
Configuration: Active(PERFORMDB_MCP)   Platform: Active(MCP)   Configuration Manager...

DASDL

Addresscheck Required	DMSII Default
Keycompare Required	False
Locked File	False
Lock Program	False
Audit Sections	0
Statistics Location	
Dump Encrypt Type	None
Obfuscate Level	0
Data Encryption Type	None
SensitiveData	
Statistics	
Reapply Completed/Independent Trans	
$-Options (DASDL Compiler)	
Internal DASDL Options	
Allowedcore	500000

Support for DMS II Secure Administration

- SensitiveData
  - Scrubs file areas before they are reused by the system
  - Supported as of AB Suite 7.0
  - Segment Configuration property
- LogAccess
  - Causes data access to be logged in the s
  - Basic option implemented in AB Suite 5.0
    - Logs all accesses for Ispec classes with “Log
  - Enhanced granularity option implemented
    - Logs all accesses for Ispec classes with “Log
      - Value can be ALL, (DM Verb List), or ALL EXCEPT
      - For example, (FIND,CREATESTORE,DELETE) or ALL EXCEPT (DELETE)



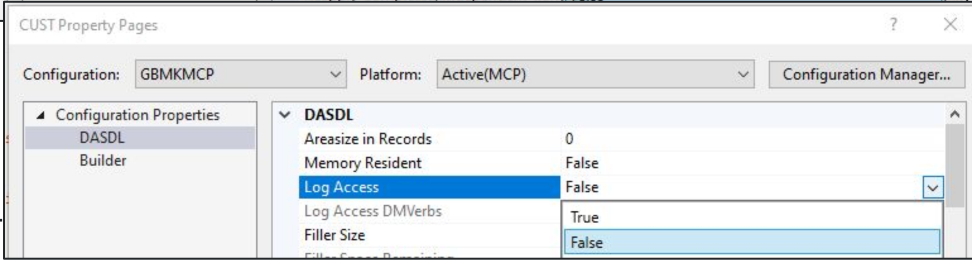
CUST Property Pages

Configuration: GBMKMCP   Platform: Active(MCP)   Configuration Manager...

- Configuration Properties
  - DASDL
  - Builder

DASDL

Areasize in Records	0
Memory Resident	False
Log Access	True
Log Access DMVerbs	ALL
Audit Sections	0
Statistics Location	
Dump Encrypt Type	None
Obfuscate Level	0
Data Encryption Type	None
SensitiveData	False
Statistics	True
Reapply Completed/Independent Tran	False



CUST Property Pages

Configuration: GBMKMCP   Platform: Active(MCP)   Configuration Manager...

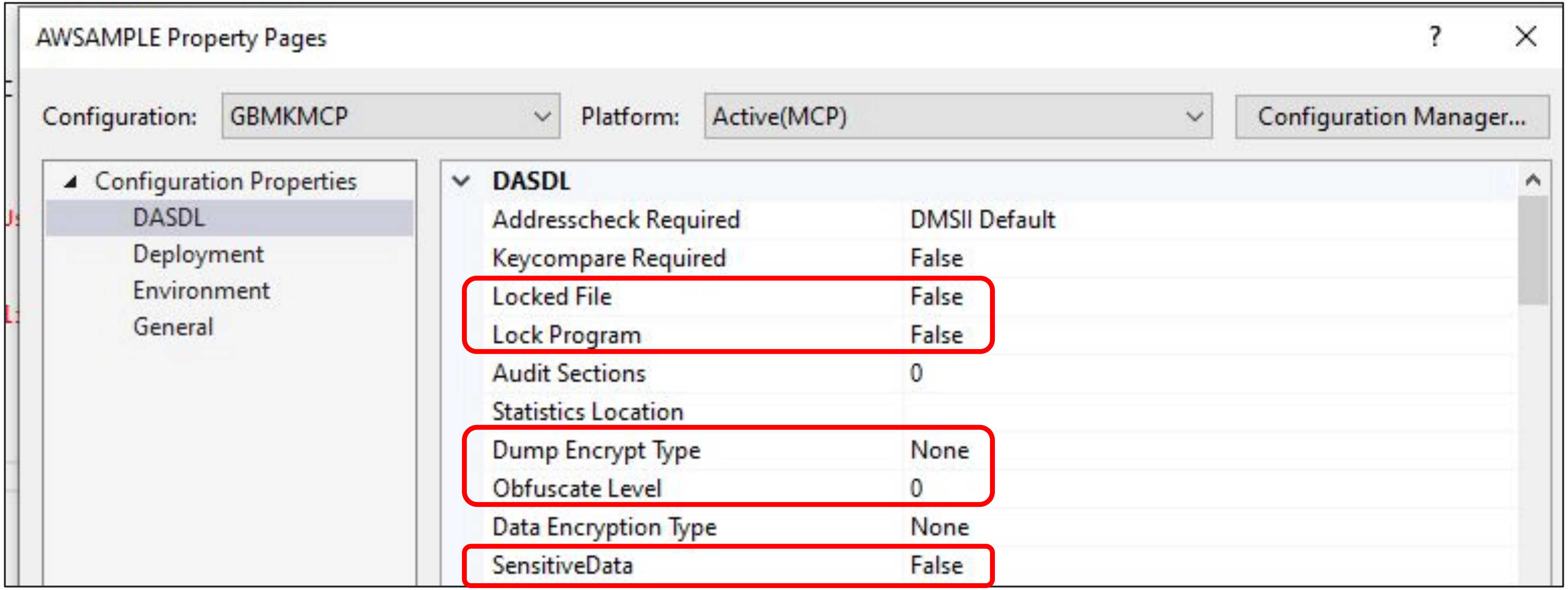
- Configuration Properties
  - DASDL
  - Builder

DASDL

Areasize in Records	0
Memory Resident	False
Log Access	False
Log Access DMVerbs	True
Filler Size	False

Support for DMS II Secure Administration

- Other features implemented in AB Suite 5.0



AWSAMPLE Property Pages

Configuration: GBMKMCP Platform: Active(MCP) Configuration Manager...

- Configuration Properties
  - DASDL
  - Deployment
  - Environment
  - General

DASDL

Addresscheck Required	DMSII Default
Keycompare Required	False
Locked File	False
Lock Program	False
Audit Sections	0
Statistics Location	
Dump Encrypt Type	None
Obfuscate Level	0
Data Encryption Type	None
SensitiveData	False

  - Prevents inadvertent manual termination of the stack

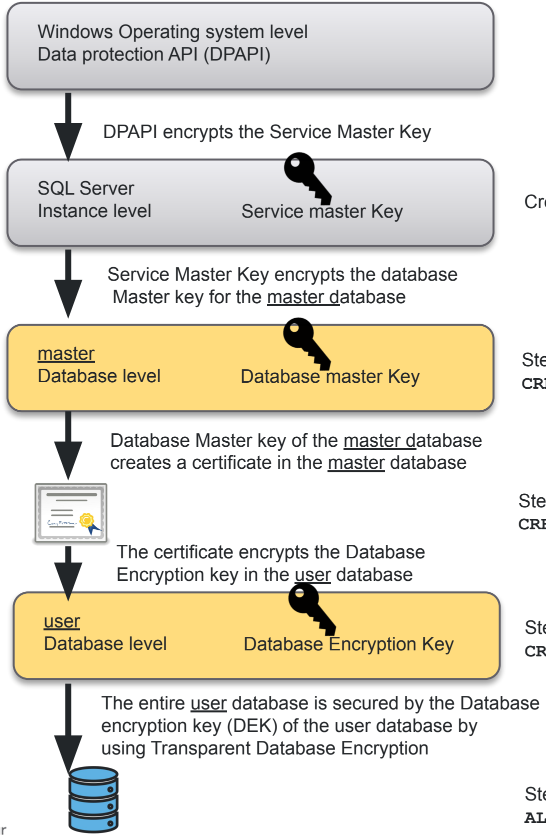
UNISYS | Securing Your Tomorrow®

Windows Runtime Features

SQL TDE

- AB Suite 8.0 Windows runtime supports SQL Server TDE
- TDE - Transparent Data Encryption
  - Used to protect Data at Rest
  - Encrypt data and transaction log files
  - Available in Standard and Enterprise edition 2019
    - Only Enterprise editions prior to 2019

SQL TDE Hierarchy – It’s Always Been Possible



Windows Operating system level
Data protection API (DPAPI)

DPAPI encrypts the Service Master Key

SQL Server
Instance level

Service master Key

Service Master Key encrypts the database
Master key for the master database

master
Database level

Database master Key

Database Master key of the master database
creates a certificate in the master database

The certificate encrypts the Database
Encryption key in the user database

user
Database level

Database Encryption Key

The entire user database is secured by the Database
encryption key (DEK) of the user database by
using Transparent Database Encryption

Created at time of SQL Server setup

Step 1 Statement:

```
CREATE MASTER KEY ….
```

Step 2 Statement:

```
CREATE CERTIFICATE ….
```

Step 3 Statement:

```
CREATE DATABASE ENCRYPTION KEY ….
```

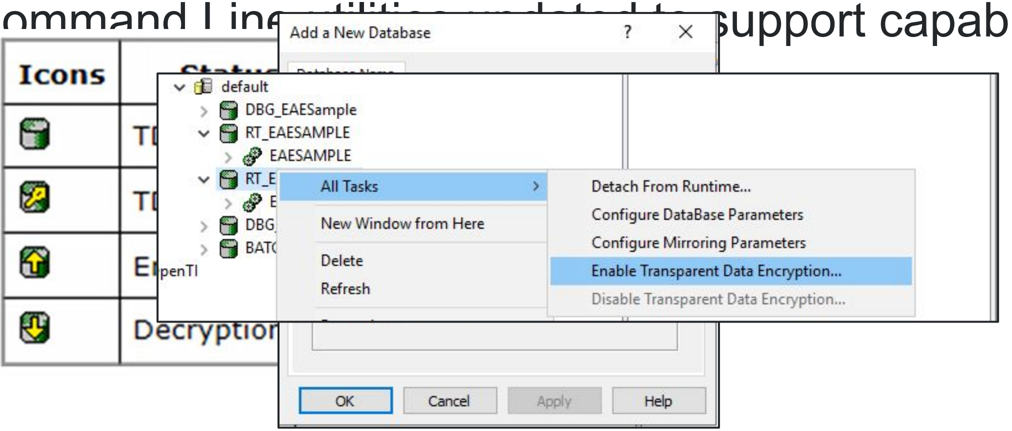
Step 4 Statement:

```
ALTER DATABASE … SET ENCRYPTION ON ….
```

Manually perform the 4 steps

AB Suite Windows Runtime Database with TDE

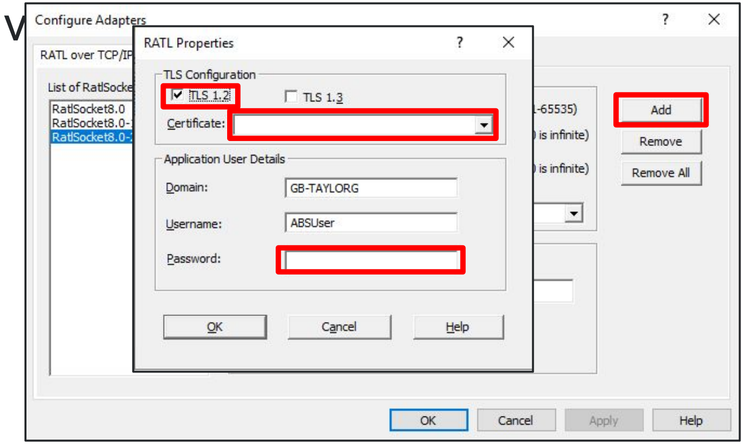
- Support of TDE by AB Suite 8.0 protects user data at rest
  - Supported by both Standard and Enterprise editions of SQL Server 2019
- Can by enabled at DB creation or modified later
  - Supports multiple AES algorithms
- AB Suite Admin Tool and Command Line utilities updated to support capability
  - Check box at DB creation
  - Option to convert existing
  - New Icons introduced to indicate state of database



UNISYS | Securing Your Tomorrow®

Secure RATL

- Provide Data in Motion security for RATL connections to Windows
  - New in AB Suite 8.0
- Only TLS 1.2 supported by default
  - TLS 1.3 is still considered experimental, not advised to use for Production
- Configuration as part of Install, via Admin Tool, or v
  - Ability to convert from TLS to non-TLS or vice versa
- Via Admin Tool => Configure Adaptors



Configure Adapters

RATL over TCP/IP

List of RatlSocke

RatlSocket8.0
RatlSocket8.0-
RatlSocket8.0-

RATL Properties

TLS Configuration

☑ TLS 1.2 □ TLS 1.3

Certificate:

Application User Details

Domain: GB-TAYLORG

Username: ABSUser

Password:

Unisys | Securing Your Tomorrow®

Conclusion

In Conclusion …

- We recognise your need – often driven by regulatory and/or audit requirements – to protect sensitive data
- AB Suite Runtime platforms offer many security features to address this need
- AB Suite increasingly leverages the security features of the respective Runtime platforms
  - And will continue to do so where opportunities arise
  - Look for an article on Single Sign On (SSO) in the upcoming Developing Agility newsletter
- AB Suite enables and simplifies the implementation of the Runtime platform security features you choose to use

Thank You