Ask the Expert

Security Changes Affecting SAS Systems

Darrell Barton, Software Development Engineer in Test
Tony Brown, Distinguished Software Performance Engineer

Darrell Barton

Software Development Engineer in Test

Darrell has more than 30 years of experience and has held many roles at SAS, including in technical support, marketing, R&D and education. Darrell has primarily been involved in the installation, support, management and administration of SAS environments. That includes working at the intersection of SAS with the operating systems and databases. As an educator, he taught classes on SAS installation, SAS administration and SAS grid administration and is a certified SAS administrator. Currently he tests the SAS®9 installation and deployment management tools, including SAS Deployment Wizard and SAS Deployment Manager.

Tony Brown

Distinguished Software Performance Engineer

Tony conducts software performance testing on a broad variety of hardware virtualizations, servers, storage types and networks. He jointly tests and works with operating systems, file systems, hardware and third-party vendors to ensure SAS performance on their platforms and software.

Tony globally supports SAS system customers' performance on reporting and analysis, statistical modeling, vertical solutions, SAS Grid Manager, and SAS Cloud Analytic Services on the SAS® Viya® platform. He provides SAS performance architecture advice for on-premises and cloud-based solutions.

Security Changes Affecting SAS Systems

Security Chanes Affecting SAS Systems

Acknowledgements

This presentation is a culmination of the dedicated work of many SAS Contributors:

R&D

Joe Hatcher, Melissa Zwirblia, Robin Crumpton

Chris Nance, Chris Smith, Darrell Barton, & Many Others

Technical Support

Tim Braam

Esther Burwell

SAS Documentation and Publications Team

Security Changes Affecting SAS Systems

Future Security Changes – Cryptographic Libraries

- Beginning with SAS 9.4 M8 SAS Foundation servers *use the Open Cryptographic libraries provided by the operating system o*n which SAS is deployed.
- The SAS Web Server is built on Apache Web Server and supports one version of OpenSSL.
- Beginning with SAS 9.4 M8, SAS delivers OpenSSL 3.0.x for use by the SAS Web Server.
- Likewise, the SAS Web Infrastructure Platform Data Server (the middle-tier Shared Services database) is build on
- The Postgres database and is delivered with Open SSL 3.0.x.
- Red Hat Linux 9.5 is deployed with OpenSSL 3.2.2
- Beginning in Red Hat Linux 9.5 the SAS NETENCRALG system option must be set to SSL.
- Because of the OpenSSL library changes, to enable FIPS, you must set NETENCRALG=SSL to specify the use of the TLS protocol for encrypted data-in-motion communications.
- SAS is providing the ability to configure TLS during Installation for the Middle-Tier starting in SAS 9.4 M9.
- In addition, beginning with PostgreSQL version 14 or later, if FIPS is enabled then the hashing functions that are required for authentication are routed to OpenSSL and must be *SCRAM-SHA-256*.
- Beginning with SAS 9.4 M9, Multi-Factor Authentication (MFA) for the Middle Tier and support of
- IBM Z Multi-Factor Authentication will be supported. In a future SAS 9.4 M9 update later this year,
- MFA support will be added for the SAS Server tier.

Security Changes Affecting SAS Systems

First, Let's Talk
About the
WHAT

Security Changes Affecting SAS Systems

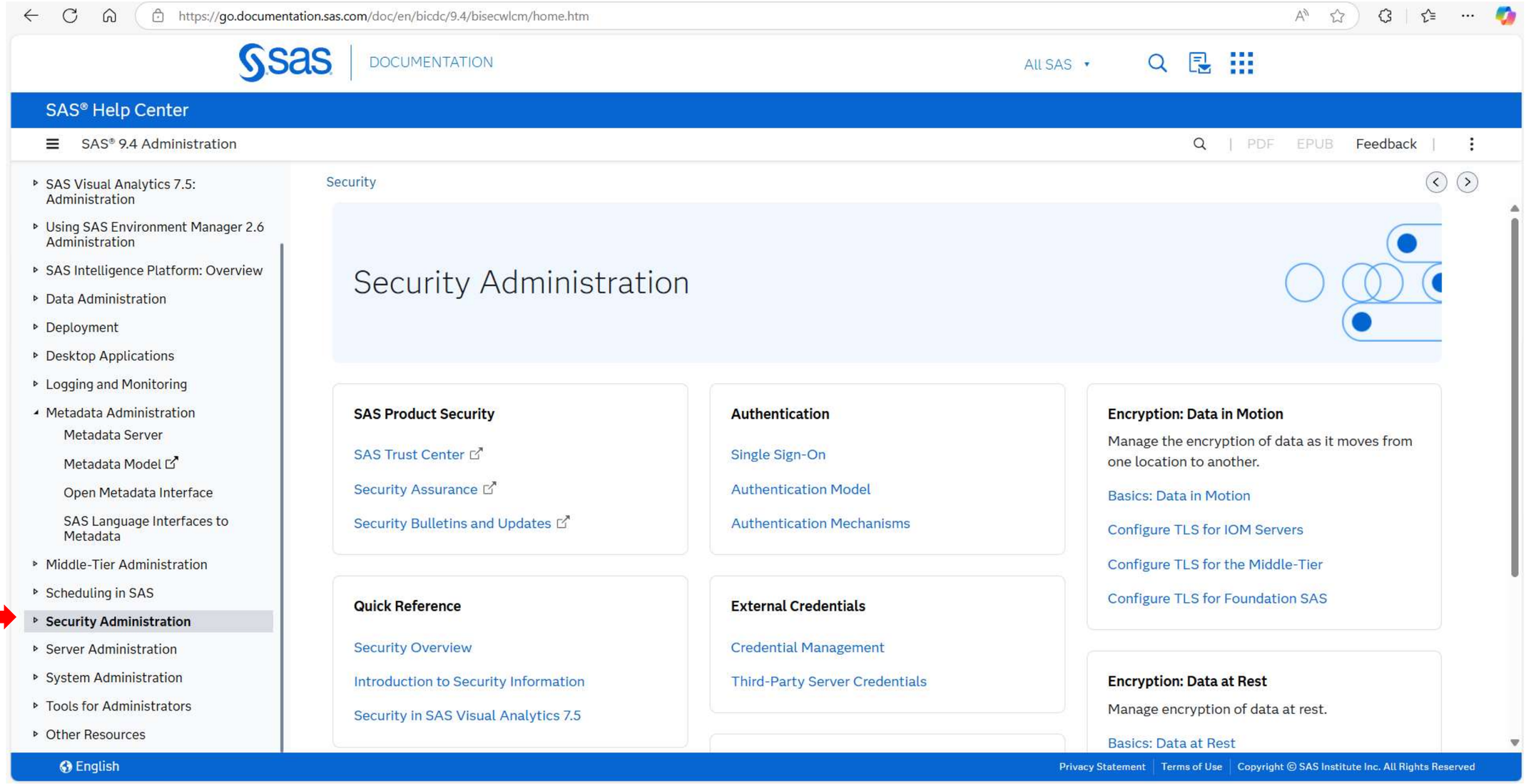
Agenda - **WHAT**

- SAS 9.4 M8 Changes
  - Encryption Changes for SAS 9.4 M8 and Forward
  - Encryption Types and Classes
  - Data Encryption at Rest
  - Data Encryption in Motion

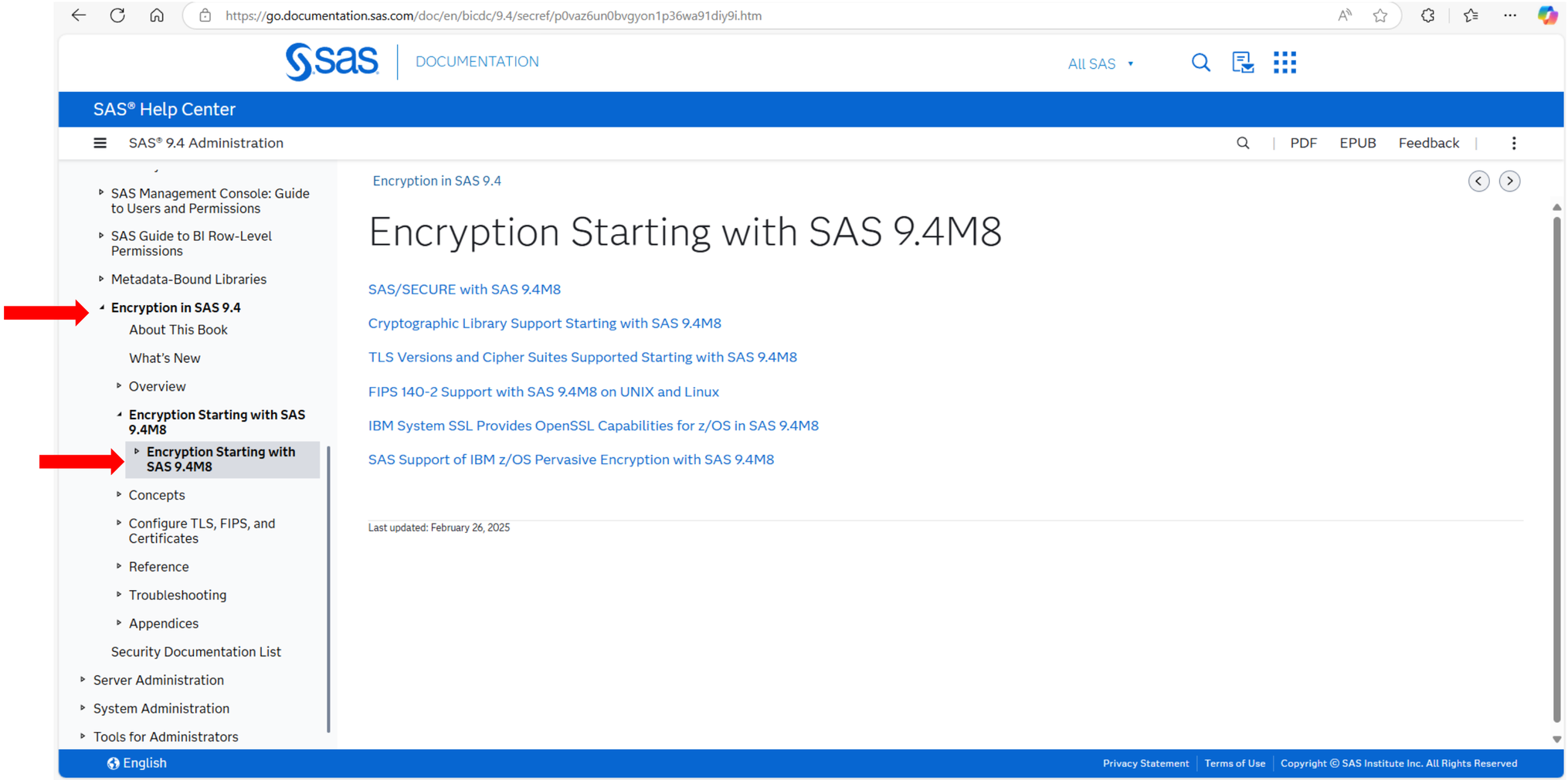
- Red Hat Linux (RHEL) 9.5 Encryption Library Changes
  - OpenSSL Version Changes from 3.1 to 3.2
  - Change in the SAS use of AES for Data in Motion

- FIPS Enablement Changes for SAS
  - OpenSSL 3.2.2

Security Changes Affecting SAS Systems



Security Changes Affecting SAS Systems



Security Changes Affecting SAS Systems

Encryption Changes for SAS 9.4 M8 and Forward

For all supported operating systems:
- TLS 1.3 support
- SAS Foundation uses OS-installed Cryptographic Libraries
- FIPS 140-2 support

For UNIX & LINUX

- OpenSSL3
- OpenSSL 1.1.1
- **!!Note** – Red Hat Linux 9 and Later, OpenSSL 3.2.2 May Exhibit Installation Errors with SAS, we will show you how to Install Successfully.

For z/OS

- Beginning in SAS 9.4 M8 and Forward, we use the IBM System SSL to support TLS. IBM also supports FIPS.

For MS Windows

- Beginning in SAS 9.4 M8 and forward, we us the Schannel SSP (Security Support Provider) Libraries
- TLS, Bcrypt

*For more information, see Cryptographic Library Support Starting with SAS 9.4M8 in *Encryption in SAS*.

Security Changes Affecting SAS Systems

Encryption Types – Quick Review

SAS basically provides encryption coverage in two contexts:

- DATA AT REST - the emphasis is on protection of passwords in configuration files and in the metadata repository. You can also encrypt SAS data sets.
  - See: SAS Help Center: Encryption for Data at Rest
- DATA IN MOTION - the emphasis is on protection of passwords in transit. You can also protect all traffic in transit among SAS Integrated Object Model (IOM) servers and SAS desktop clients.
  - See: SAS Help Center: Encryption for Data in Motion
- COST – There is a performance cost to encryption. SAS/SECURE traditionally has been very low cost, but deep levels of industry protocol data and communications encryption can slow things down.

Security Changes Affecting SAS Systems

Encryption Classes - Proprietary and Industry Standard

SAS Proprietary Encryption

Data At Rest
- SAS Proprietary Data Encryption

Data In Motion
- SAS Proprietary Communications Encryption

Industry Standard Encryption

Data At Rest
- AES

Data In Motion
- TLS (SSL)

9.4 M7 and Previous

9.4 M7 and Previous
- SAS Provided Cryptographic Libraries via SAS/SECURE
- SAS/SECURE is included in all orders
- Obsolete NETENCRALG options can be used, but NETENCRALG = SSL is strongly recommended

9.4 M8 and Forward

- SAS Foundation servers use OS-Installed Cryptographic Libraries
- Obsolete NETENCRALG options can be used, but NETENCRALG = SSL is strongly recommended
- June 2025, 94M9 SDW screens will no longer surface obsolete NETENCRALG options
  - Moving to TLS (SSL) for Encryption for Data in Motion
  - NETENCRALG options are present in M9 and can be set in configuration files, but NETENCRALG = SSL is strongly recommended
- In first quarter 2026, NETENCRALG=SSL (TLS) will become the only supported option Hot fixes will remove obsolete NETENCRALG options 94M7/94M8/94M9
  - Must transition to NETENCRALG = SSL after hot fixes are installed

** For All SAS 9.4 M8 Encryption Changes see: SAS Help Center: What's New

Security Changes Affecting SAS Systems

Encryption for Data at Rest

Storage Context		**Encoding Available**
Login Password and SASPASSWORD Objects On disk in the metadata	→	SAS Proprietary Encoding (AES256, 16& 64bit Salt (or+ additional hash iterations).
Internal account password on disk in the Metadata	→	SHA256-10000, SHA256, or MD5 hashing
Password on disk in a configuration file	→	SAS Proprietary Encoding (AES256, 16& 64bit Salt (or+ additional hash iterations).

Security Changes Affecting SAS Systems

Encryption for Data in Motion

- IOM Server to Client – Encryption algorithms and SSL Protocol (SAS Proprietary Encoding, (RC2, RC4, DES, TRIPLEDES, AES, SSL)
  - TLS (SSL) is Very Highly Recommended NOW, and will be REQUIRED in SAS 9.4 M9
  - ONLY SSL (TLS) NETENCRALG options will be supported in updates to be delivered after the initial release of SAS 9.4M9.
- OTHER IN MOTION – Some Systems Implement None, or USE TLS
  - Metadata Server to LDAP
  - Web Server to Web Application Server
  - Web Browser to Web Server
  - SAS Deployment Agent Traffic
  - SAS Environment Manager to Agent Server Traffic
  - SAS Environment Manager to Agent Traffic

** For All SAS 9.4 M8 Encryption Changes – see : SAS Help Center: What's New

Security Changes Affecting SAS Systems

Red Hat Linux 9.5 Encryption Changes

Beginning in Red Hat Linux (RHEL) Release 9:

- The Host Provided SSL Library Supports OpenSSL 3.2.2 and supports TLS 1.3 and TLS 1.2
- Starting in SAS 9.4 M9 or later, NETENCRALG=AES is no longer supported for Data in Motion in RHEL 9.5. Only NETENCRALG=SSL is supported on RHEL 9.5
- For FIPS mode, set -encryptfips and -netencralg=SSL (plus cert info)

Security Changes Affecting SAS Systems

FIPS 140-2 Enablement for SAS 9.4 M8 and Forward – UNIX & LINUX

Previously

- SAS Delivered the OpenSSL Libraries
- We documented How to build the FIPS Enabled Libraries and Install Them
- We documented the use of the ENCRYPTFIPS System Option to enable FIPS with SAS
- This placed SAS in FIPS Mode

Going Forward (9.4 M8 and On)

- SAS Now Can use the OpenSSL Libraries installed on the Host Operating System
- FIPS is enabled by the Operating System for the Host (SYSADMIN must install)
- The SAS ENCRYPTFIPS System Option enables SAS in the FIPS Mode
- Currently an installation blip on enabling FIPS! Discussed later in this presentation

*See your Operating System Documentation on FIPS 140-2 Certification Enablement

*See Encryption Examples in SAS Help Center: Encryption for Data in Motion

Security Changes Affecting SAS Systems

Now, Let's Talk About the HOW

Security Changes Affecting SAS Systems

Agenda - **HOW**

- SAS 9.4 M8 Changes
  - Configuring OpenSSL for SAS 9.4 M8
- FIPS Enablement Changes for SAS
  - Configuring SAS OpenSSL for FIPS enablement
    - SAS Deployment Wizard
- TLS Certificates
- Manual FIPS Configurations for Servers and Spawners
    - IOM Servers
      - Metadata & OLAP Servers
      - Object Spawners
      - Connect Spawners
    - Middle Tier Servers

Security Changes Affecting SAS Systems

How To: SAS 9.4 M9 TLS Certificates & TLS (SSL) Enablement

- TLS requires the use of Certificates!!!
- SAS 9.4 Ships with a root trusted Certificate Library as a starter
- Please Read: SAS Help Center: About Certificates, as certificates can be Sourced from many different providers

- SAS will use the SSL Libraries installed and enabled on the OS
  - SAS Help Center: Using Operating System OpenSSL Libraries with SAS 9.4M9
- OpenSSL library versions that are supported and tested with SAS 9.4M9 are OpenSSL 3, OpenSSL 1.1.1, and OpenSSL 1.0.2.
- When the Red Hat Enterprise Linux 9 operating system is installed with OpenSSL 3.2.2, You must install hot fix https://tshf.sas.com/techsup/download/hotfix/HF2/L8X.html#71068 with SAS 9.4 M8, if you haven't already - to avoid the following installation error:
  - ERROR: The OpenSSL library (libssl) cannot be located

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 FIPS Enablement

- Prior to SAS 9.4 M9 , SAS delivers OpenSSL libraries for use by SAS and documents how to build FIPS enabled libraries and install them. Setting the ENCRYPTFIPS system option enables FIPS and places the SAS software in FIPS mode.
- Starting with SAS 9.4 M9, the cryptographic libraries that support FIPS must be installed on the operating system and FIPS must be enabled on the operating system. The ENCRYPTFIPS system option is then set to ensure that the SAS software is placed in FIPS mode.
- The following link in the SAS 9.4 Administration Guide gives detailed information on FIPS 140-2 SSL Library acquisition and usage on the OS:
  - SAS Help Center: How to Use FIPS 140-2 Capable OpenSSL Libraries with SAS 9.4 M9 on UNIX and Linux
- Due to changes in the underlying security libraries used by Red Hat Release 9 (RHEL9), the configuration of SAS 9.4 M8 on RHEL9 **does not install properly in FIPS mode**. Note, the steps shown in

The following slides do not apply to Red Hat releases prior to RHEL9.

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Check to see if FIPS Mode is enabled on the OS

Linux

For FIPS environments, verify whether the OS in FIPS mode:

```
$ fips-mode-setup --check
FIPS mode is enabled.
```

Verify that the OS has OpenSSL FIPS compliant libraries installed:

```
$ openssl version
OpenSSL 3.0.7 1 Nov 2022 (Library: OpenSSL 3.0.7 1 Nov 2022)
$ which openssl
/usr/bin/openssl
$ ldd /usr/bin/openssl | grep libssl
libssl.so.3 ⇒ /lib64/libssl.so.3 (0x00007f76663db000)
```

Security Changes Affecting SAS Systems

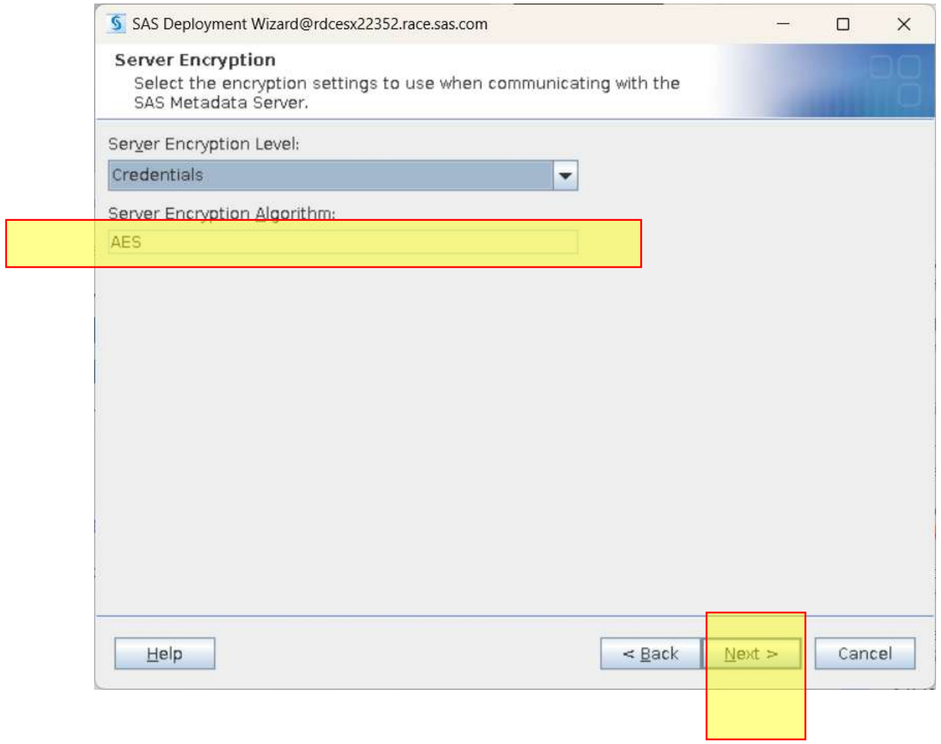
How To: SAS 9.4 M8 Deployment Wizard – FIPS Enablement Error

- There are two prompts at the core of FIPS enablement of the SAS 9 deployment shown below. An issue has arisen deploying SAS 9 in FIPS enabled systems when using the intuitive selections on the prompts.
- If "Configure SAS server to use FIPS-certified encryption algorithms" is selected on screen one when configuring the metadata server and SAS Web Infrastructure Platform, the only option when selecting an algorithm on screen two is **AES**. This causes an error during configuration as shown below. To avoid this error, you must keep the ***Configure SAS server to use FIPS-certified encryption algorithms*** option **unchecked** and use the SAS Proprietary algorithm. Manual steps are then taken to secure the SAS 9 environment.

Screen 1 – Enable FIPS-Certified Encryption Algorithms

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Deployment Wizard – FIPS Enablement Error



Screen 2 – AES Server Encryption

The messages in the log file referenced in the error indicate there is a problem with the keys.

- [echo] getmetadatavalues exception: Error connecting to metadata server, using host ‘host.org.com' port '8561' user 'cfgsas1' repository 'Foundation'. Exc: 'com.sas.metadata.MdException: An exception was thrown during the encryption key exchange.

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Deployment Wizard – FIPS Enablement Error

- Leave Enable FIPS-certified Encryption Algorithms unchecked !!
- We will manually configure the various Servers later….

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Reminder: TLS Requires Certificates

Certificates are used in the TLS authentication process and *are also* prerequisite for installing SAS 9 to be FIPS compliant. They are generated by a trusted third party, a *certificate authority*, that acts as a central point to validate the person or organization is who they claim to be. Instead of paying an external trusted certificate authority for a globally acceptable certificate, certificates can be self-signed or site-signed for internal usage within an organization. SAS accepts all three types of certificates,

1. Self-signed
2. Site-signed
3. Third-party-signed

For a FIPS compliant environment:

- Self-signed certificates are **not accepted.** SAS requires certificates and their associated keys to be FIPS compliant.
- There are many ways to generate certificates, aside from the ones that ship with SAS. Please refer to the documentation based on your environment for more information. For more complete information on TLS Certificates please see:

Configure TLS Certificates and FIPS on UNIX and Linux

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Metadata & OLAP Servers Manual TLS Configuration IOM Servers

To configure the SAS Metadata and SAS OLAP servers for FIPS involves adding options to the **sasv9_usermods.cfg** file for the server. This is a user modifiable extension to the **sasv9.cfg**. The sasv9.cfg is built at deployment time and ***should not*** be modified. It is processed first and then calls the sasv9_usermods.cfg file to process the options found there. Note, the values for options in sasv9_usermods.cfg are processed last during server start up and override those found in sasv9.cfg.

The sasv9_usermods.cfg file can be found in these directories,

- Metadata server - <Config>/Lev1/SASMeta/MetadataServer
- OLAP server - <Config>/Lev1/SASApp/OLAPServer

**Note: The _usermods.cfg files are preserved on upgrade in place.

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Metadata & OLAP Servers Manual TLS Configuration IOM Servers

The following options need to be added to each of these files. Be sure to make a backup before editing.

- **-netencryptalgorithm "SSL"** or **netcncralg "SSL"** (quotes are shown but are optional) – Either of these forms will override the SAS Proprietary algorithm selected during configuration prompting and found in the sasv9.cfg file.)
- **-sslcertloc=<Path*>** - specifies the location of a file that contains a digital certificate for the machine's public key. This is used by servers to send to clients for authentication. **NOTE – In TLS Support for IOM Servers there is a : instead of an =.**
- **-sslpvtkeyloc=<Path*>** - specifies the location of the file that contains the private key that corresponds to the digital certificate that was specified by using the SSLCERTLOC= option. **NOTE – In TLS Support for IOM Servers there is a : instead of an =.**
- **-sslpvtkeypass="*password*"** – specifies the password that TLS requires in order to decrypt the private key. The private key is stored in the file that is specified by using the SSLPVTKEYLOC= option. **NOTE – In TLS Support for IOM Servers there is a : instead of an =.**

* Path is typically referring to the SAS Security Certificate Framework directory, <SASHOME>/SASSecurityCertificateFramework/#.#/.

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Metadata & OLAP Servers Manual TLS Configuration

IOM Servers

Example User Configuration File:

```
/*
 * sasv9_usermods.cfg
 *
 *   This config file extends options set in sasv9.cfg.  Place your site-specific
 *   options in this file.  Any options included in this file are common across
 *   all server components in this application server.
 *
 *   Do NOT modify the sasv9.cfg file.
 *
 */
-netencryptalgorithm "SSL"
-sslcertloc="/install/SASHome/SASSecurityCertificateFramework/1.1/servercert.pem"
-sslpvtkeyloc="/install/SASHome/SASSecurityCertificateFramework/1.1/serverkey.pem"
-sslpvtkeypass="MySecret12345!"
```

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 OBJECT and CONNECT Spawners Manual Configuration

IOM Servers

[illegible] launch scripts can be found in these directories:

- Object spawner – <Config>/Lev1/ObjectSpawner/ObjectSpawner_usermods.sh
- Connect spawner – <Config>/Lev1/ConnectSpawner/ConnectSpawner_usermods.sh

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 OBJECT and CONNECT Spawners Manual Configuration IOM Servers

- Go to the configuration folder of the Object Spawner:
  <Configuration directory>/Lev<n>/ObjectSpawner
- Edit the ObjectSpawner_usermods.sh file for Object Spawner_usermods.sh file
- Add the following to the Object Spawner script:

```
CERT_HOME=${SAS_HOME}/SASSecurityCertificateFramework/1.1
CERT_LOC=${CERT_HOME}
/server.pem CERT_KEY=${CERT_HOME}/serverkey.pem
CALIST_LOC=${CERT_HOME}
/cacerts/trustedcerts.pem
USERMODS="${JREOPTIONS} -sslpvtkeyloc ${CERT_KEY}
-sslcertloc ${CERT_LOC} -sslcalistloc ${CALIST_LOC}"
```

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 OBJECT and CONNECT Spawners Manual Configuration

IOM Servers

- Go to the configuration folder of the Connect Spawner:
  <Configuration directory>/Lev<n>/ConnectSpawner
- Edit the ConnectSpawner_usermods.sh file for Connect Spawner_usermods.sh file
- Add the following to the Connect Spawner script:

```
CERT_HOME=${SAS_HOME}/SASSecurityCertificateFramework/1.1
CERT_LOC=${CERT_HOME}/server.pem CERT_KEY=${CERT_HOME}/serverkey.pem
CALIST_LOC=${CERT_HOME}/cacerts/trustedcerts.pem USERMODS_OPTIONS=“
-sslpvtkeyloc ${CERT_KEY} -sslcertloc ${CERT_LOC}
-sslcalistloc ${CALIST_LOC}"
```

Security Changes Affecting SAS Systems

How To: SAS 9.4 M8 Middle-Tier Servers TLS Configuration

Complete Instructions to Configure the Middle-Tier for TLS can be found at:

- SAS Help Center: Transport Layer Security (TLS) and Middle-Tier Servers

And more specifically for Web Servers:

- SAS Help Center: Configure TLS for SAS Web Server Manually
- Note: The SAS Web Server can be configured for TLS at the initial deployment…

Security Changes Affecting SAS Systems

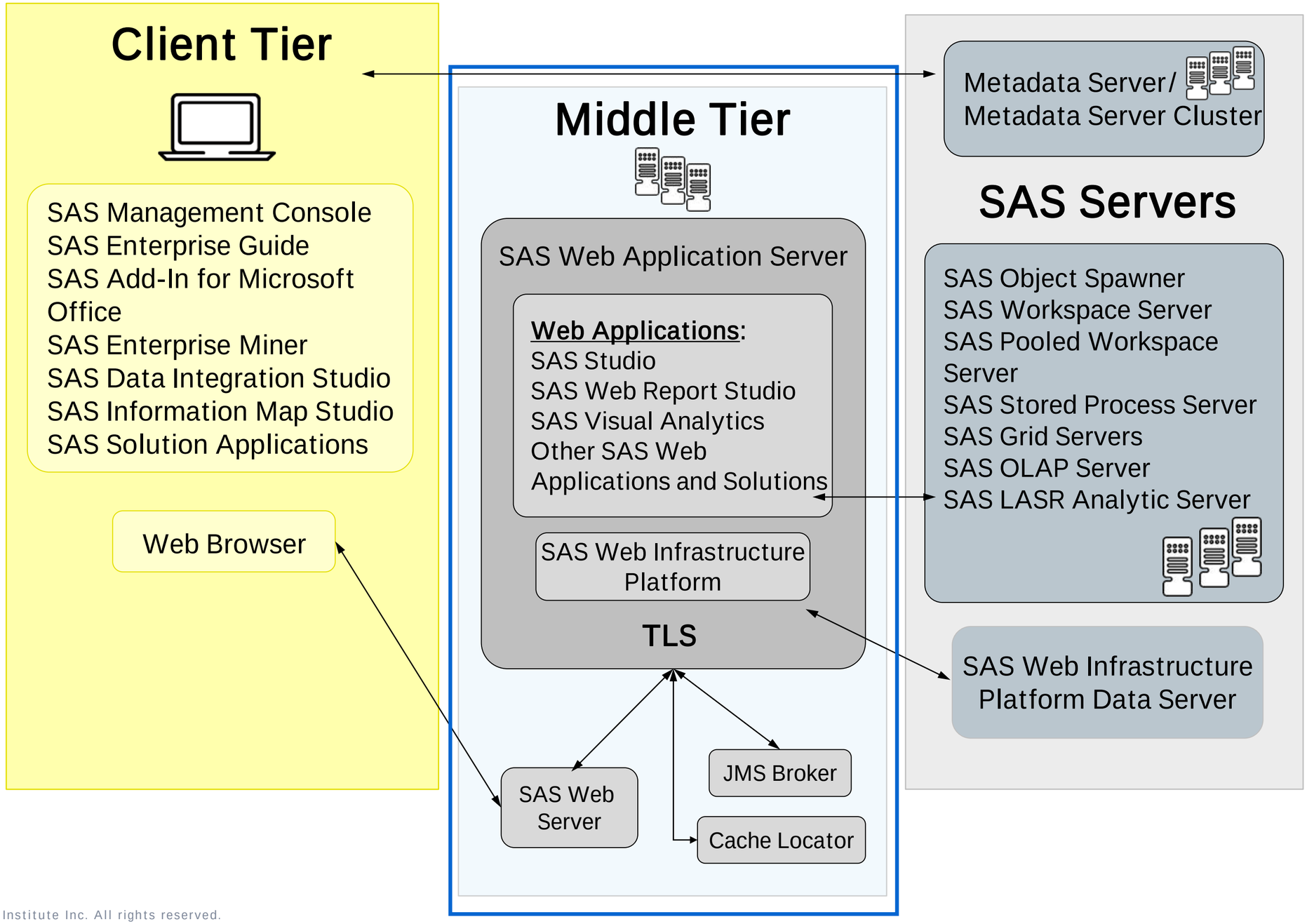
How To: PostgreSQL Version 14 and OpenSSL Hashing

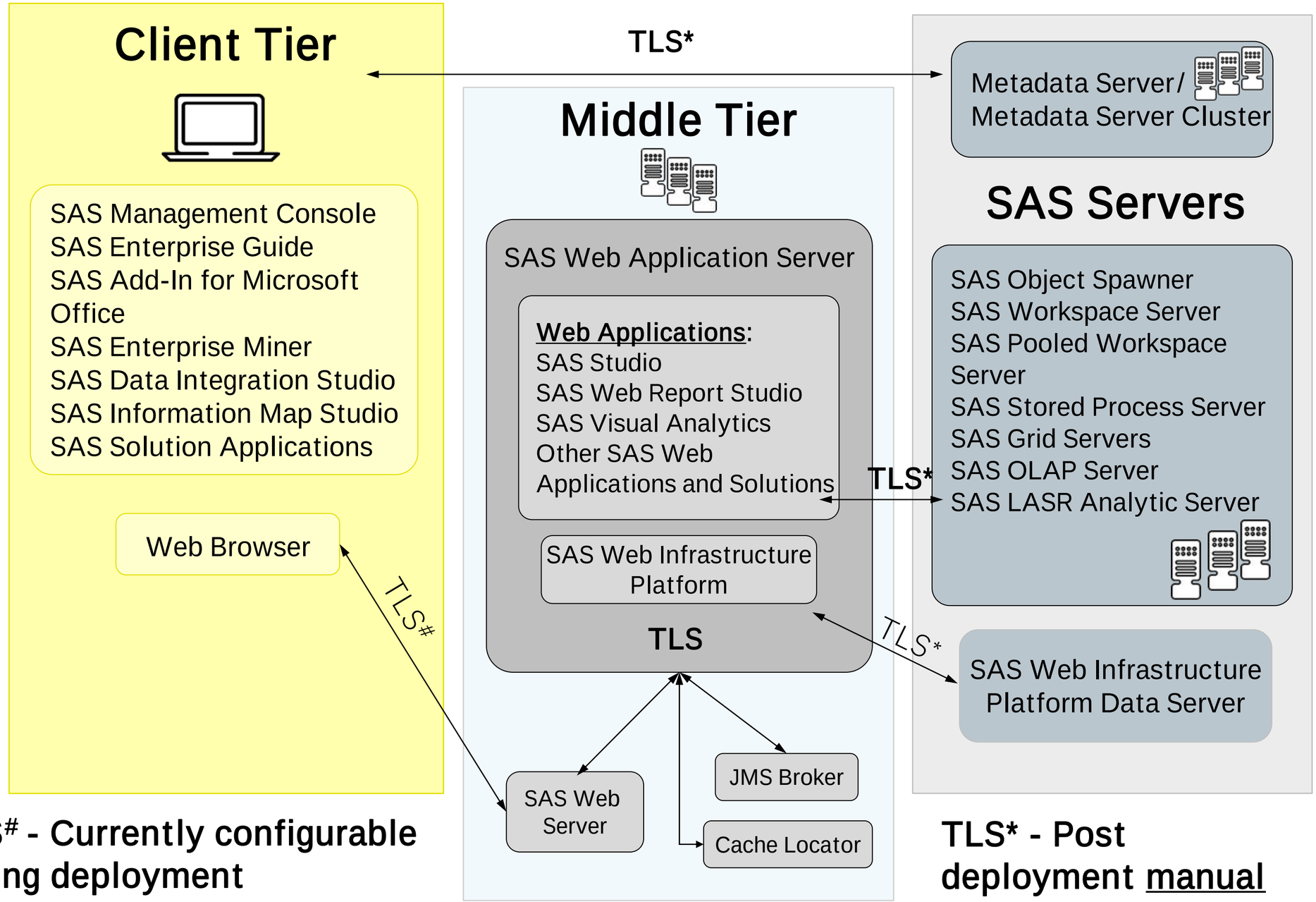
- Beginning with PostgreSQL Version 14 or later, if FIPS is enabled then the hashing functions that are required for authentication are routed to OpenSSL and **MUST** be SCRAM-SHA-256.
- See: SAS Help Center: FIPS 140-2 Compliance

Security Changes Affecting SAS Systems

Future Enhancements

- SAS is creating the following enhancements and support:
  - Automate the configuration to use TLS in future releases
  - In future releases of SAS9, support of Multi-Factor Authentication (MFA) will be available:
    - SAS Middle Tier
    - SAS Server Tier
    - Mainframe - uses a solution separate from other Unix and Windows hosts which supports IBM Z Multi-factor Authentication





TLS# - Currently configurable during deployment

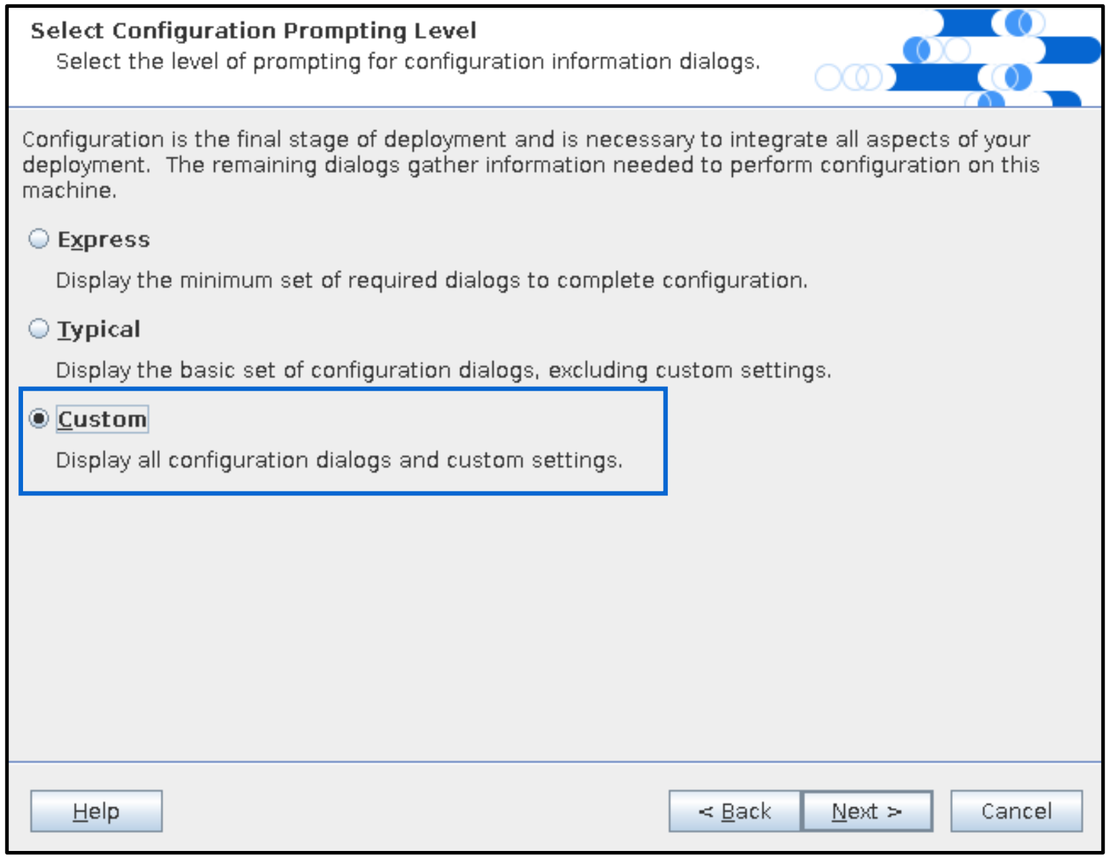
TLS* - Post deployment manual configuration

TLS Enabling the Middle-Tier

- SAS Deployment Wizard

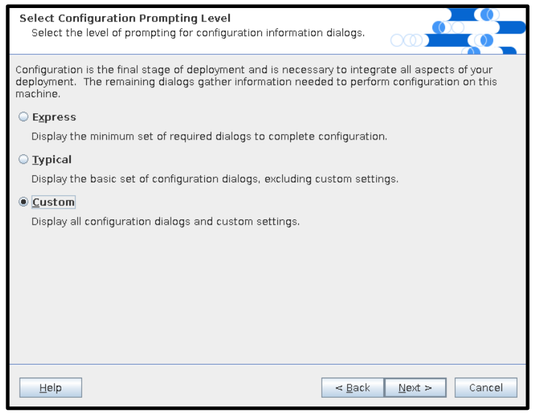
TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Select the Custom Path

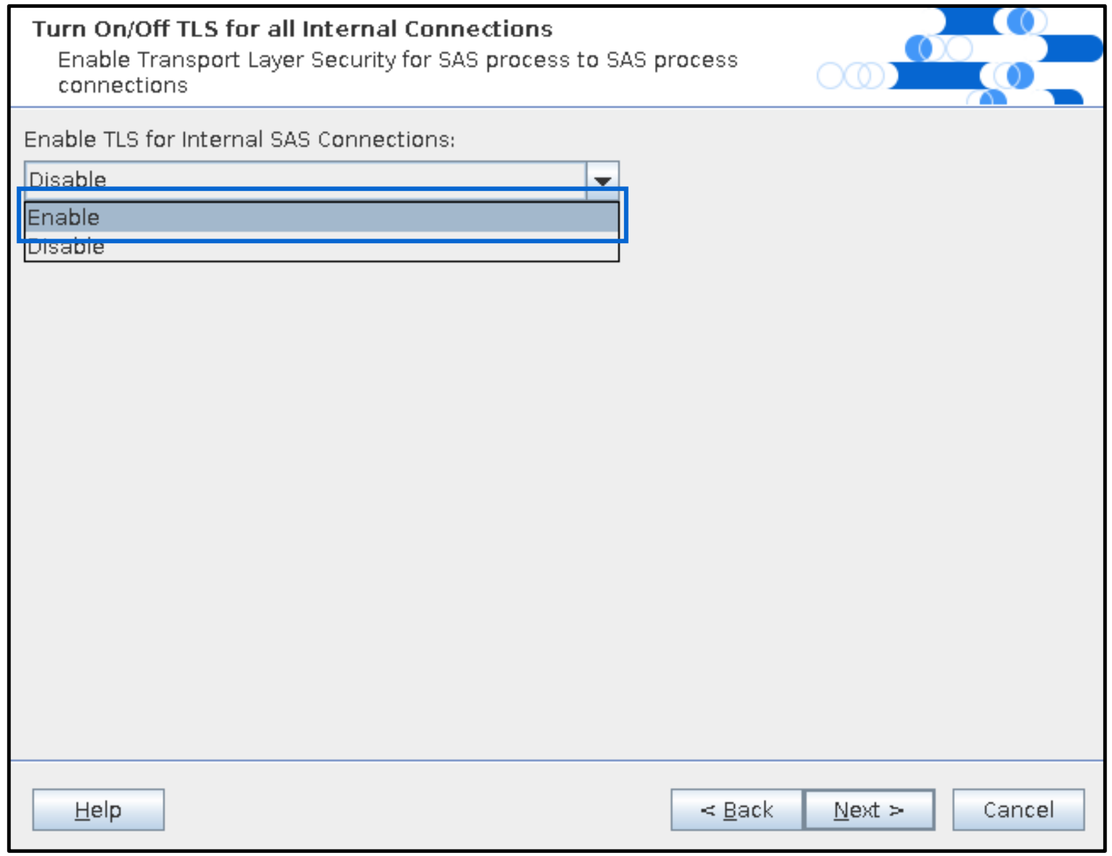


TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Enable TLS

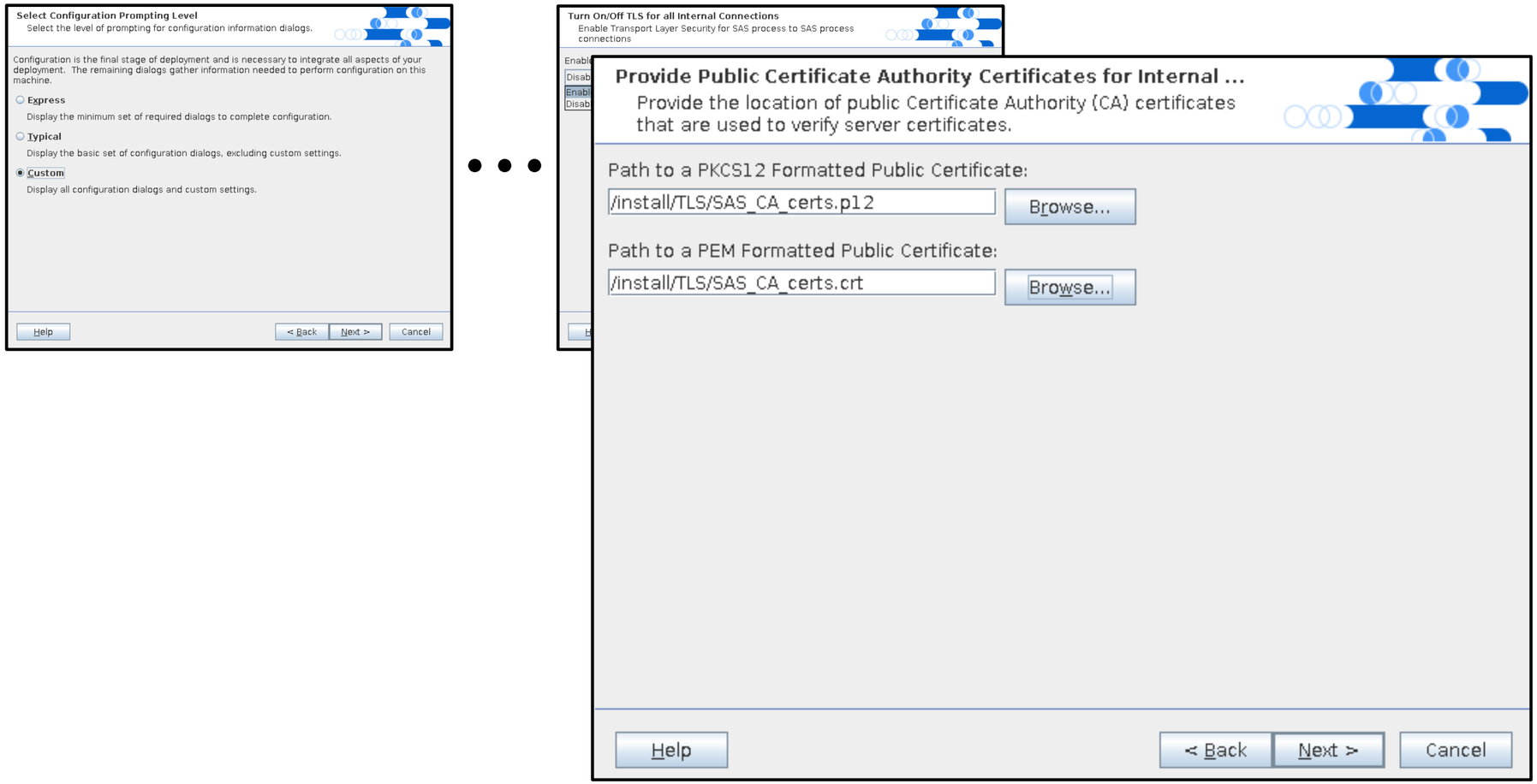


• • •



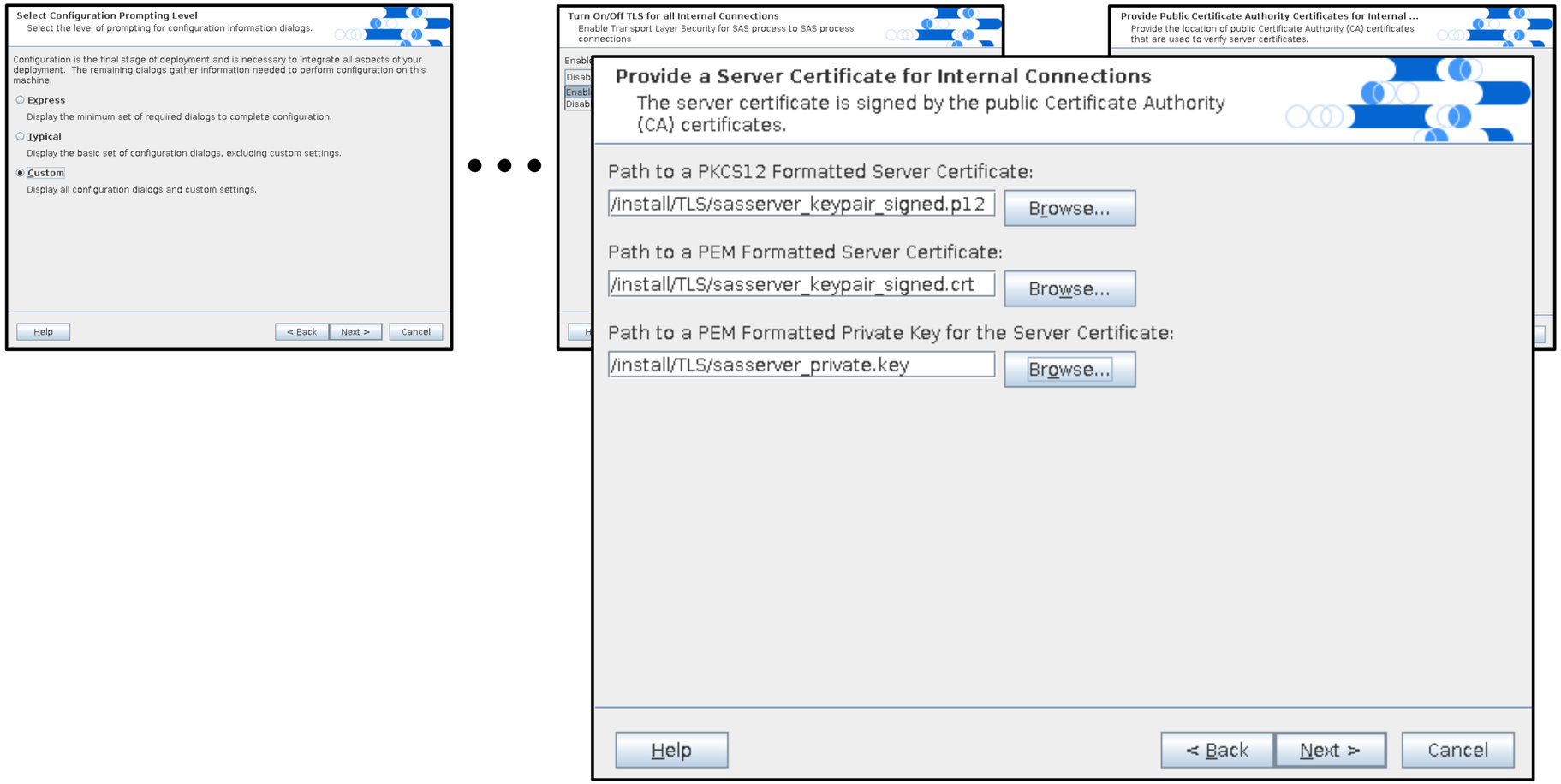
TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Select Certificate Authority Certificates



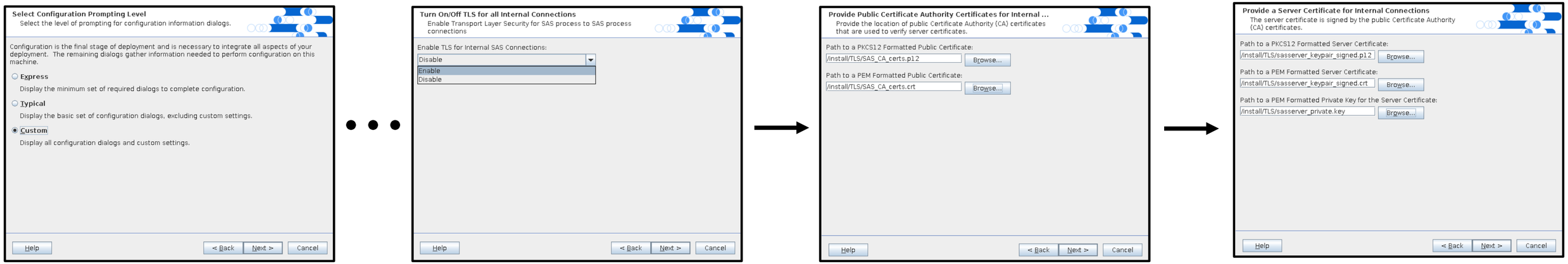
TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Select Server Certificates and Key



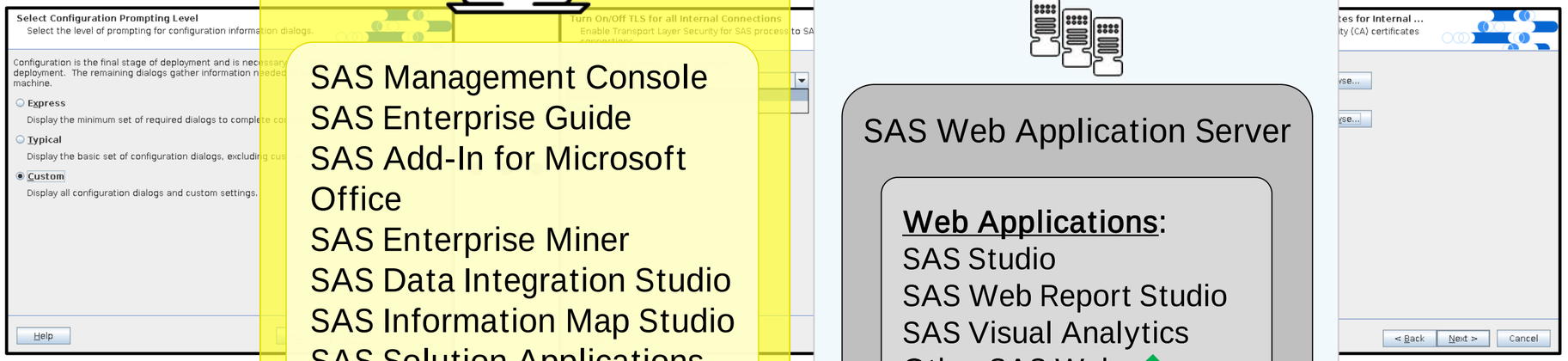
TLS Enabling the Middle-Tier

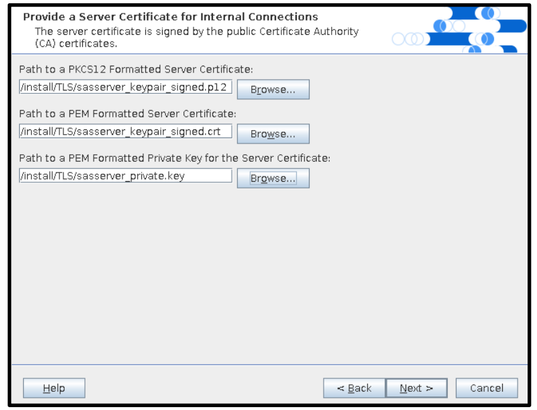
- SAS Deployment Wizard – Setting up TLS



TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Settin

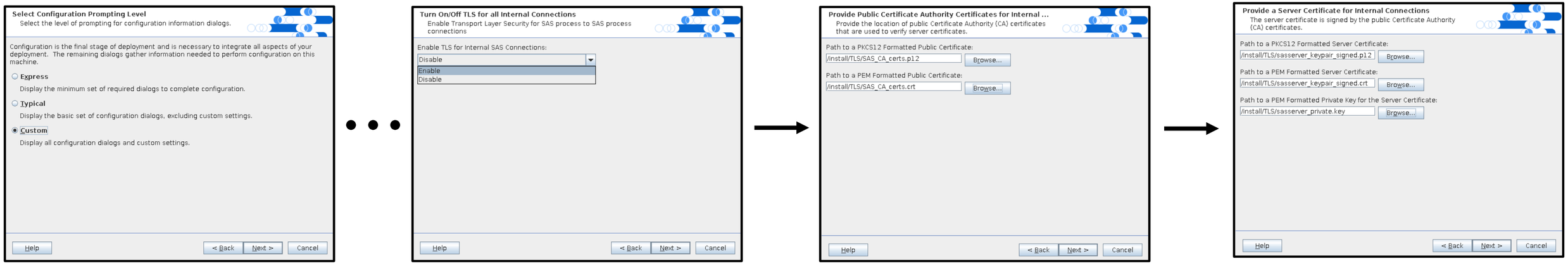




TLS# - Currently configurable during deployment

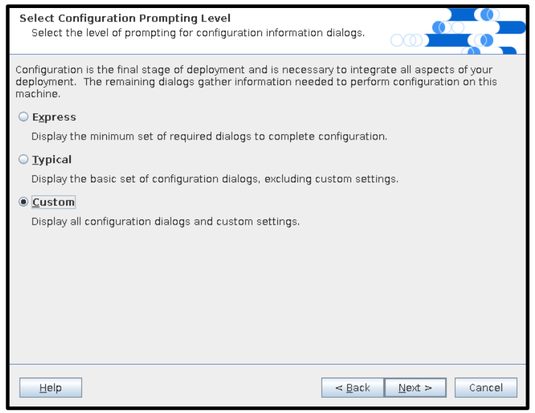
TLS Enabling the Middle-Tier

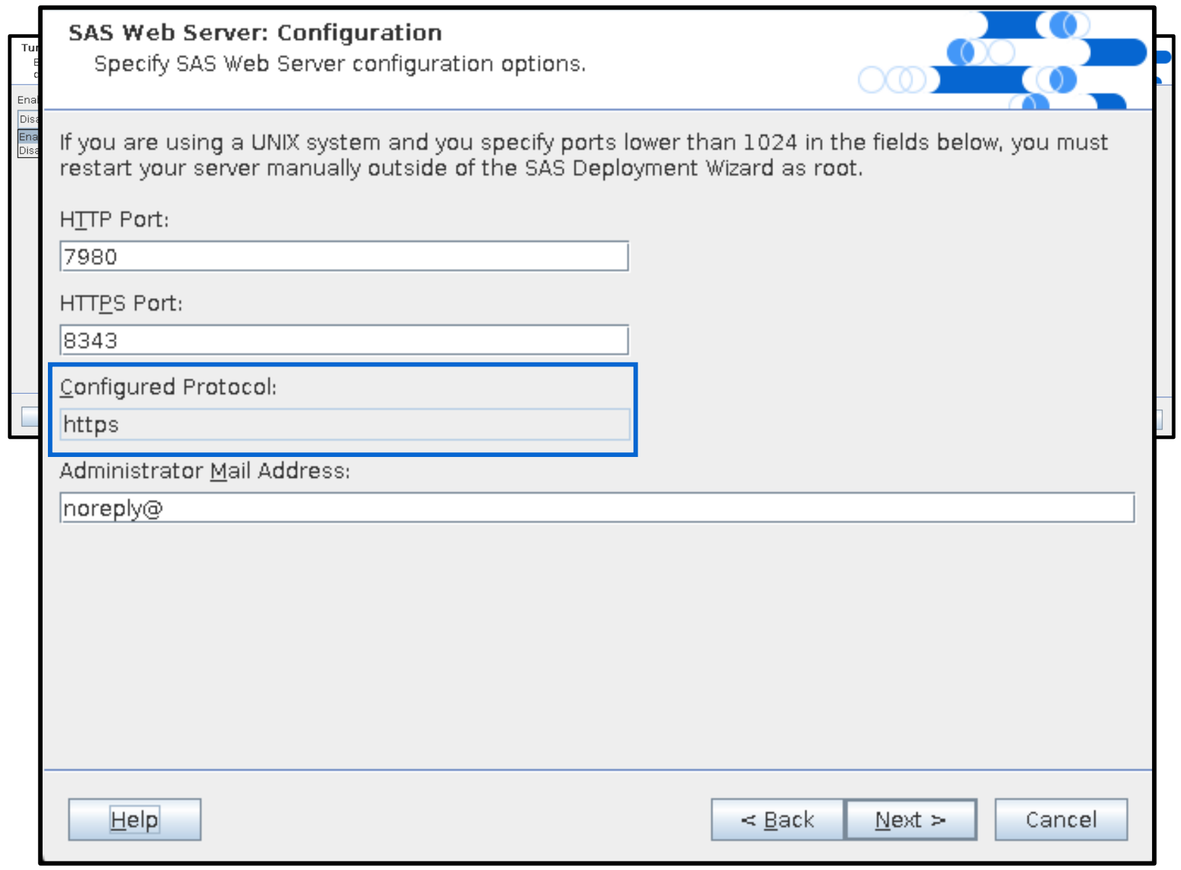
- SAS Deployment Wizard – Existing Web Server TLS setup

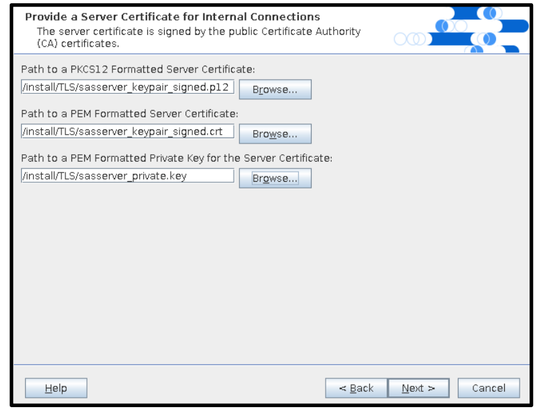


TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Existing Web Server TLS setup

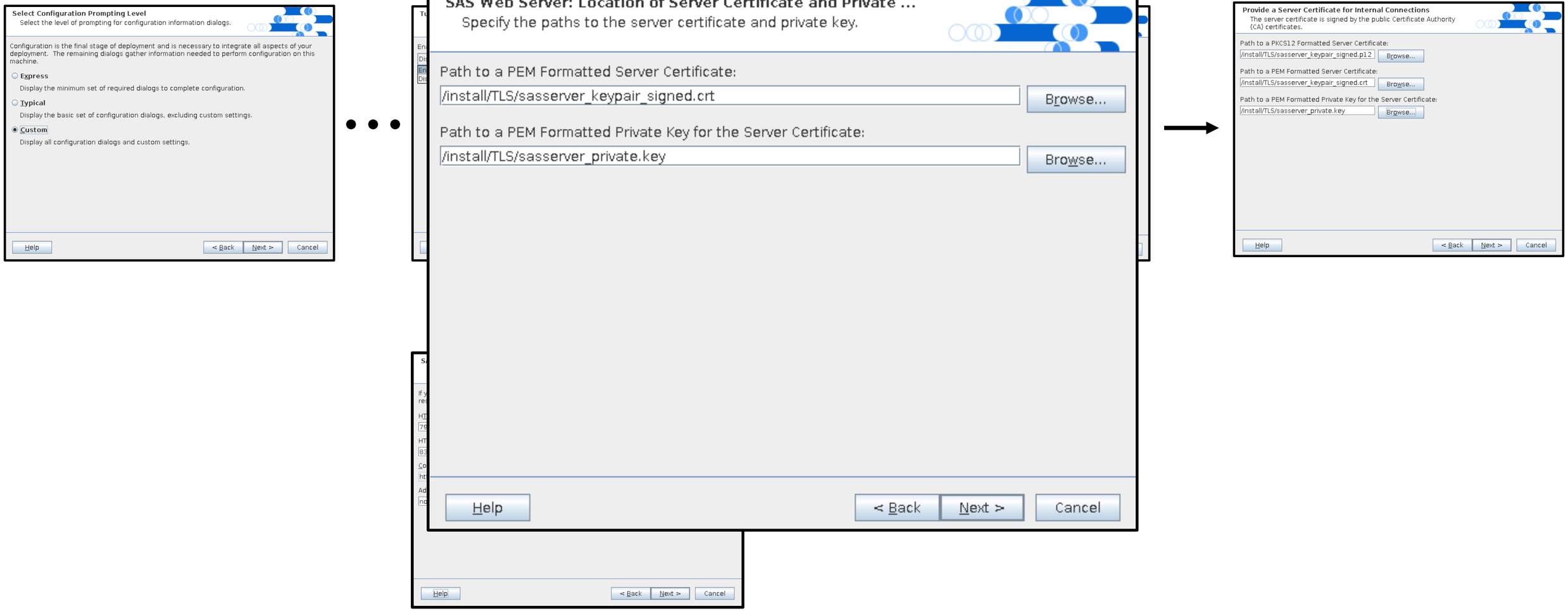






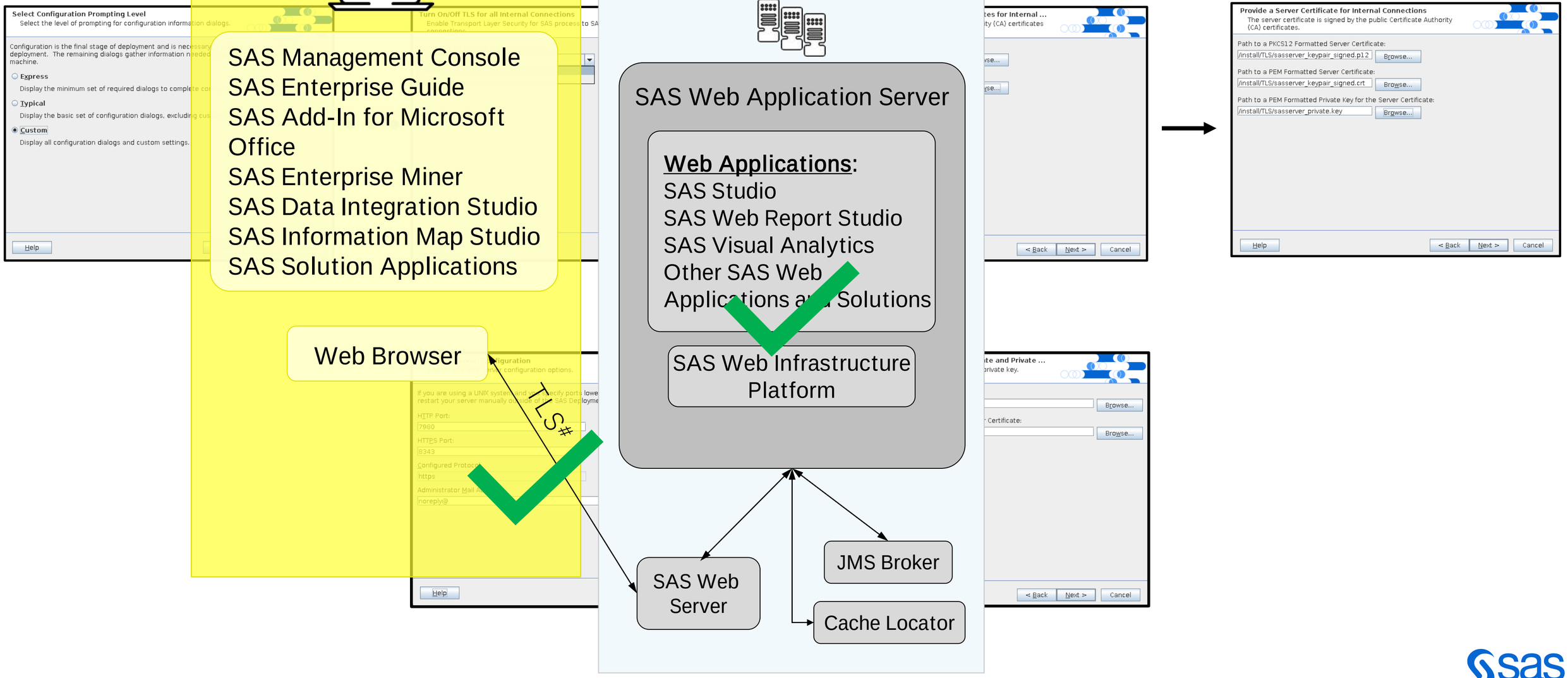
TLS Enabling the Middle-Tier

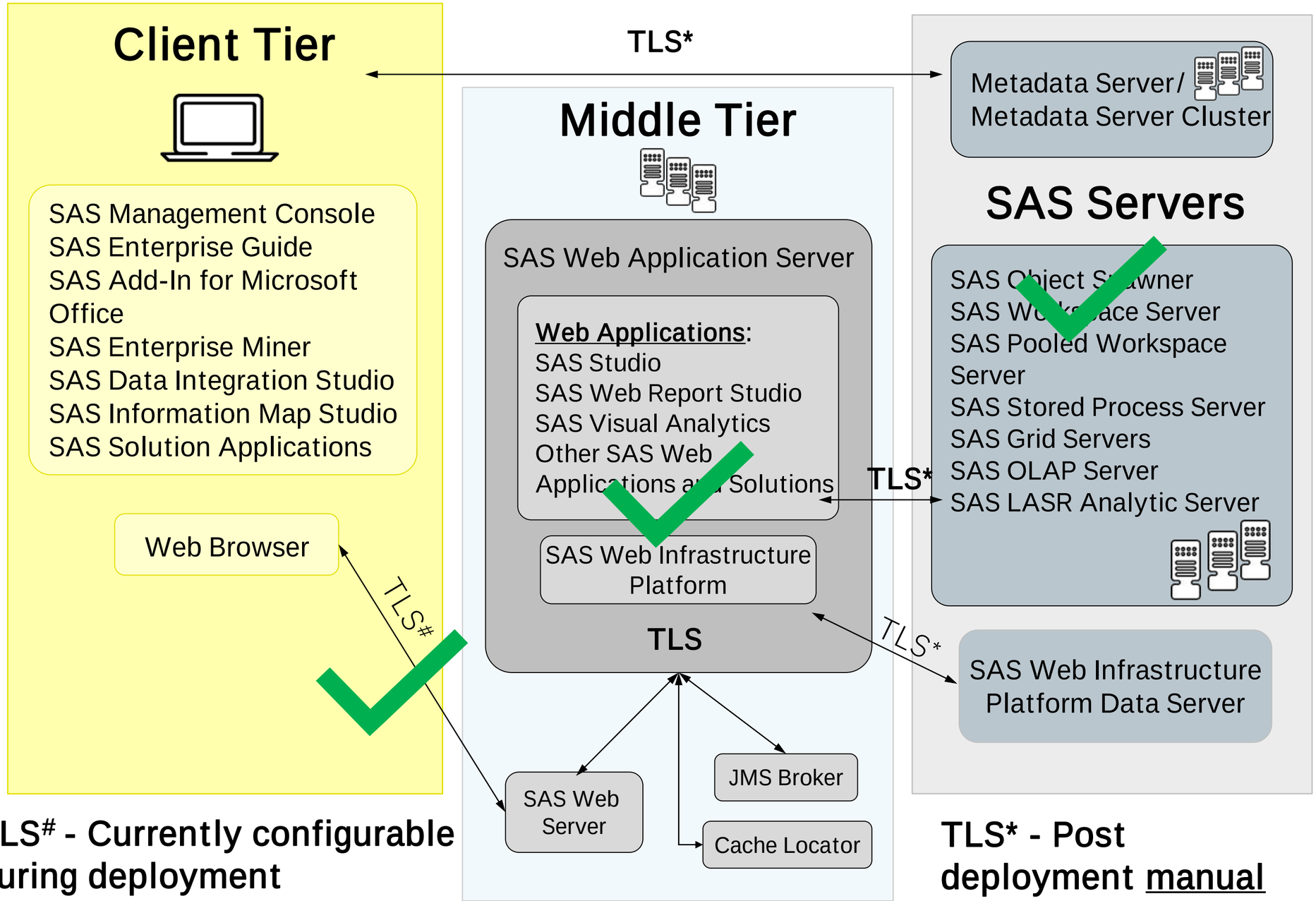
- SAS Deployment Wizard – Existing Web Server TLS setup



TLS Enabling the Middle-Tier

- SAS Deployment Wizard – Existing Setup





TLS# - Currently configurable during deployment

TLS* - Post deployment manual configuration

Security Changes Affecting SAS Systems

Questions?

Explore Helpful Resources

[Ask the Expert]
View other user webinars that provide insights into using SAS products to make your job easier.

[FREE Training]
Learn from home – free for 30 days. Get software labs to practice and online support if needed.

[SAS Support Communities]
Ask questions, get answers and share insights with SAS users.

[SAS Analytics Explorers]
An exclusive platform to collaborate, learn and share your expertise. Gain access to a diverse network to advance your career. Special rewards and recognition exclusively for SAS users.

[SAS Users YouTube Channel]
A plethora of videos on hundreds of topics, just for SAS users.

[Newsletters]
Get the latest SAS news plus tips, tricks and more.

[Users Groups]
Meet local SAS users, network and exchange ideas – virtually.

[SAS Profile]
If you haven't already done so, create your SAS Profile to access free training, SAS Support Communities, technical support, software downloads, newsletters and more.

Thank you for joining us for this SAS webinar.