vPRO™ Security FAQ

Security FAQ for Intel® vPro™ Technology

New content will be added as new FAQs are identified.

Table of Contents

Security of Provisioning and Configuration

- Advantage of using MTLS over TLS in an Intel® AMT configuration profile
- Difference between TLS for Intel AMT provisioning and TLS for Intel AMT Out Of Band (OOB) Management
- Difference between Digest and Kerberos authentication in Intel AMT configuration profile
- Choosing between TLS-PSK and TLS-PKI
- Risk of not using TLS
- Certificates for Intel AMT initial provisioning
- Certificates for Intel AMT management
- Security of Intel AMT-based web service
- Access controls of vPro activated machines
- How an end user can change Intel AMT configuration
- Role-based Security for Intel AMT management

Value Added Security Features of Intel vPro Technology

- NAC profile
- 802.1X profile
- Certificates supporting security of AMT machines production connections
- Whether System Defense can replace Anti-Virus and Personal Firewall

#

1. What is the advantage of using MTLS over TLS in an Intel AMT configuration profile?

When an Intel AMT machine is configured with a TLS profile, it is acting like a TLS/SSL – enabled server, which provides for traffic encryption and integrity and for the Intel AMT machine authentication. Connecting party (management console or Web client) authenticates only with its password or Kerberos credentials. MTLS (TLS with mutual authentication), in addition to the security provided by TLS, requires the connecting party to authenticate with its PKI client certificate, and that certificate should be successfully verified and validated by the Intel AMT machine. So, MTLS provides an additional layer of security by requesting a connecting party to authenticate both with its password or Kerberos credentials and with its trusted client certificate. It is strongly recommended for AMT-enabled laptops which may be exposed to additional risk outside an enterprise network.

#

2. What is the difference between TLS for provisioning and TLS for Out Of Band (OOB) Management?

These are two absolutely different tunnels supported by different certificates.

Enterprise provisioning of a vPro machine starts with the machine (acting as a client), sending “Hello” to a provisioning server (acting as a server) and a following authentication and sending sensitive data between those two. Provisioning server should have a pre-installed TLS certificate from a certificate authority (CA), which root certificate’s hash is installed on the machine, therefore the machine can authenticate the server and support the TLS tunnel. Using pre-shared secret instead of installing PKI certificate on the server is also possible for authentication and encryption. Although the latter case is implementing TLS-PSK protocol whilst the former is implementing TLS-PKI, both of them are providing TLS security. OOB management is originated by a management console or Web UI client to a vPro machine, which is acting as a server in this case. Therefore the TLS is enabled by the server certificate on the machine, which was requested and installed on the machine in the process of provisioning with a profile with TLS selected. If the profile has MTLS option selected, the establishing TLS tunnel will also require the management server to authenticate with its client certificate.

#

3. What is the difference between Digest and Kerberos authentication in an Intel AMT configuration profile and what is advantage of using one above another?

Intel AMT supports two types of authentication: Kerberos and Digest. Kerberos should be used only if Active Directory (AD) and Domain Controller (DC) are available and both infrastructure users and Intel AMT devices are integrated with AD. Once an administrative user is logged in on the server, he can access the Intel AMT device based on his group membership in AD and according to his access permissions and realms. The advantage of using Kerberos is that it is a Microsoft* Windows integrated authentication which does not require to store and maintain credentials on Intel AMT devices or a console. The main disadvantage is that it requires tight integration with AD and current versions of ISV's configuration servers should be checked to see if they require AD schema modification.

Digest is a more secure password authentication method, where a client presents a digest (hash) of its credentials and a nonce (timestamp and random number) to the server. It prevents sending credentials over the wire in clear text during authentication. User's credentials however may need to be stored in clear on the AMT device for authentication process. The main advantage of this authentication is that it does not require AD and DC integration. The disadvantages are the burden of maintaining authentication credentials and potentially lower security.

#

4. When can a user choose between TLS-PSK and TLS-PKI? What is the difference and advantage of using one above another?

Both TLS-PSK and TLS-PKI are providing authentication and network encryption between Intel AMT machines and Provisioning server for Intel AMT enterprise provisioning. TLS-PSK requires generating a pre-shared secret key (PSK) for each Intel AMT platform's UUID and securely distribute it between provisioning server and each of the Intel AMT machines. So, it does require at least one "touch" to the machine to be provisioned. TLS-PKI needs just a server certificate installed on the provisioning server and that certificate should be issued by a trusted Certificate Authority (its root certificate hash is pre-installed on each machine).

TLS-PKI provisioning is available starting with AMT 2.2, 2.6 and 3.0 and is also called Remote Configuration (RCFG) or Zero-Touch Configuration (ZTC). Learn more by reading the Remote Configuration FAQ.

#

5. What is the risk of not using TLS?

Both authentication credentials and data between configuration/management console or web client and an Intel AMT machine is traversing network in a clear text and may be eavesdropped. Also, a rogue machine may be put on a network to receive profiles with credentials from the configuration console.

#

6. NAC profile can be configured for a vPro machine. What is it for?

It is an optional feature and is not required with initial provisioning of vPro machines.

vPro machines support Network Admission Control (NAC), which provides network security on the data link level. It means that a NAC-enabled network device validates a security posture message of a connecting client machine as soon as network connectivity and power are on. The machine's security posture, to be acceptable and trusted by the network device, should be digitally signed by a trusted certificate and configured in the NAC profile, which needs to be installed on the vPro platform.

#

7. 802.1X profile can be configured for vPro machine. What is it for?

It is an optional feature and is not required with initial provisioning of vPro machines.

vPro machines support 802.1X network authentication standard, which provides network access control on the data link level. It means that an 802.1X -enabled network device authenticates a connecting client machine as soon as network connectivity and power are on. A specific authentication protocol and certificates used for mutual authentication when implementing 802.1X, are configured in the 802.1X profile.

#

8. How many certificates are used for initial provisioning and what are they?

There are three PKI certificates used just for provisioning of a vPro device:

- Provisioning Web Server Certificate. Installed on provisioning server for TLS secure console / Web GUI access to the server.

- Provisioning remote configuration certificate. Must be issued by a CA, which root certificate hash is pre-installed on AMT machine. Installed on provisioning server for AMT Remote / Zero touch provisioning over TLS-PKI.

- AMT trusted root certificates hash. Pre-installed on vPro devices to enable validation of provisioning servers certificates during TLS connection for remote/"zero touch" provisioning.

#

9. How many certificates are used for AMT management and what are they?

There are three (TLS) to four (MTLS) PKI certificates used just for managing an Intel AMT device:

- AMT Web service certificate. Installed during provisioning on an Intel AMT machine to enable TLS tunnel for Intel AMT management (if it is required by Intel AMT profile)

- AMT web client certificate. Installed on a Web UI machine or management console if Intel AMT configuration profile requires mutual authentication (MTLS)

- AMT trusted root CA certificate. Installed on Web UI machine or management console to allow validation of AMT Web service certificates during TLS/MTLS connection to it.

- Management Server's trusted root CA. Installed on Intel AMT during provisioning, if an Intel AMT profile requires MTLS.

#

10. What certificates are used to secure just Intel AMT machines production connections rather than connections for provisioning and managing these devices?

- NAC posture signing certificate. It is automatically generated and installed on Intel AMT devices during configuration, if an Intel AMT profile is configured with NAC option

- 802.1X authentication certificate. It is requested, automatically generated and installed on Intel AMT devices during configuratiIntel on, if an AMT profile is configured with 802.1X option

#

11. What is the security around AMT-based web service?

Web service implemented in the Intel® vPro firmware is a proprietary code developed for the sole purpose to support this chipset management. It was developed and tested following all best security practices in order to avoid, discover and eliminate any potential vulnerabilities. Access control is applied to the out of band Intel AMT connections in accordance with profile configuration. Connections and message flows can be protected with TLS or MTLS.

#

12. Can System Defense replace Anti-Virus and Personal Firewall?

No. System Defense chiefly works as a network security control in addition to available endpoint security controls. It does not provide as much granularity and flexibility as personal firewalls and does not deal with infected data or software like anti-virus does. However, as a hardware-based control, it works when software-based controls are not functional. System Defense allows the ability to isolate a machine off the network by out of band means. Also, its heuristic policies afford to detect a machine worm-like network behavior and automatically isolate or quarantine it.

#

13. What access controls protect a vPro activated laptop inside and outside enterprise network?

The machine is protected according to its configuration profile:

- access with Digest or Kerberos user authentication

- client certificate authentication, if the installed profile requires MTLS

- access only to the realms assigned to individual users

#

14. Can a laptop/desktop user change Intel AMT configuration, so it will not be possible to manage it out of band?

Yes. If an end user presses an OEM dedicated button (usually Ctrl+P) when computer boots, he can enter the Intel AMT configuration menu, which requires local admin authentication. If a user knows admin credentials, he can log in and un-provision the machine and make it unmanageable out of band.

#

15. Is there a Role Base Security for managing Intel AMT machines?

Each account or group is assigned a certain set of realms it can control. These realms dictate administrator or user privileges.

*Other names and brands may be claimed as the property of others.