

Resolve Duplicate ZTNA Device IDs in Secure Access Deployments Using SysPrep Golden Images

Contents

Issue

Multiple Windows physical machines deployed from a SysPrep golden image are generating identical ZTNA device IDs, specifically the same `ztnaDeviceId` across multiple endpoints. This duplication causes several critical problems:

- Repeated re-enrollment of devices with the same ZTNA device ID
- Public key overwrites during each re-enrollment process
- Posture check failures on all machines except the most recently enrolled device
- Access failures through Secure Access for affected endpoints

The observed behavior occurs when multiple machines in the fleet share the same ZTNA device ID, causing each enrollment to overwrite the public key of the previous machine. All machines except the latest one to enroll fail to send posture checks, resulting in access denial through the Secure Access infrastructure.

Multiple hostname and user ID pairs were identified as being linked to the same ZTNA device ID, demonstrating the scope of the duplication issue across the deployment.

Environment

- Cisco Secure Access (ZTNA implementation)
- Windows physical machines (not virtual machines)
- SysPrep golden image deployment methodology
- Windows ADK (Assessment and Deployment Kit) tools for image deployment
- ESD (Electronic Software Delivery) file format for image capture
- Standardized OS hardening process including mandatory software installation

- Standard local admin and guest account configuration

Resolution

The resolution process involved comprehensive log analysis and identification of the root cause through detailed investigation.

Identify and Resolve Root Cause

The investigation revealed that the SysPrep process was not properly generating unique device identifiers during the golden image deployment.

The analysis involved:

Examination of Windows registry keys, specifically:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

Collection of user Security Identifier information using:

whoami /user

The resolution required modifying the SysPrep process to ensure that device-specific identifiers are properly regenerated during deployment, preventing the duplication of ZTNA device IDs across multiple physical machines.

- Renewing UDID by running **dartcli.exe -nu** command changes value of Nounce under "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails" registry path.
- Deleting JSON file from C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments & restarting ZTA service unenrolls the user. You need to manually enroll the user. This generates a new JSON file without any other impact.
- Renewing UDID on all the endpoints must not have any impact as long as the value is not verified/evaluated on any servers.

1. Launch command prompt as an administrator and go to "%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART" directory.
2. Run **dartcli.exe -u** to check the value of current UDID.
3. Run **dartcli.exe -nu** command. This command renews the UDID.
4. Verify the new value by repeating the command in step 2.
5. Delete JSON file from the C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments directory
6. Restart VPN & ZTA services. At this point ZTA must be in unenrolled state.
7. Let the user manually enroll the ZTA
9. Verify the value of new ztnaDeviceId in the JSON file.

Monitoring and Validation

After implementing the corrective measures to ensure unique ZTNA device ID generation:

- Monitored the enrollment process across multiple machines
- Verified that each machine generated unique ZTNA device IDs
- Confirmed successful posture check functionality on all enrolled devices
- Validated that public key overwrites no longer occurred during enrollment

Cause

The root cause was identified as the SysPrep golden image deployment process not properly generating unique device identifiers for ZTNA enrollment. When multiple Windows physical machines are deployed from the same SysPrep golden image, certain device-specific identifiers that are used to generate the ZTNA device ID remain identical across all deployed machines.

The SysPrep process, while effective for standardizing OS configuration and software deployment, was not configured to regenerate the specific identifiers that the Cisco Secure Client uses to create unique ZTNA device IDs. This resulted in all machines deployed from the same golden image inheriting identical ZTNA

device identification parameters, leading to enrollment conflicts and authentication failures in the Secure Access infrastructure.

Related Content

- [Cisco Technical Support & Downloads](#)