DESIGN Document

Intune Documentation

Customer – St Andrews Healthcare

Peter Cashen & Nic Fuller

June 2025

# Table of Contents

Table of Contents 2

Revision History 7

Approvals 7

1. Introduction 8

2. St Andrews Intune Configuration 8

2.1. Filters 8

2.1.1. \*StAH-Win-Filter-Shared-GroupTag 9

3. Update rings for Windows 10 and later 9

3.1. Update Policies 9

4. Scripts 9

4.1. Scripts (PowerShell) 9

5. Feature updates for Windows 10 and later 9

5.1. Feature Updates 10

6. Device compliance 10

7. Windows enrollment 10

7.1. Autopilot 10

7.1.1. StAH Shared Device Entra ID Joined Self Deploying 10

8. Driver updates for Windows 10 and later 10

8.1. Templates 10

9. Tenant admin 12

9.1. Filters 12

9.1.1. \*StAH-Win-Filter-Baseline - All 12

9.1.2. \*StAH-Win-Filter-Baseline - All GroupTags 13

9.1.3. \*StAH-Win-Filter-Shared-GroupTag 13

9.1.4. \*StAH-Win-Filter-Standard GroupTag 14

9.1.5. StAH-Win-Filter-EntraID Hybrid Joined 14

9.1.6. StAH-Win-Filter-EntraID Joined 15

10. Update rings for Windows 10 and later 15

10.1. Update Policies 15

10.1.1. Win - Updates - U - Update Ring - Broad Ring - v1.0 15

10.1.2. Win - Updates - U - Update Ring - Pilot Ring - v1.0 16

10.1.3. Win - Updates - U - Update Ring - Preview Ring - v1.0 17

11. Scripts 18

11.1. Scripts (PowerShell) 18

11.1.1. Remove-Bloatware 18

11.1.2. Windows 11 v3.0.1 Services CIS L2 23

12. Feature updates for Windows 10 and later 26

12.1. Feature Updates 26

12.1.1. Win - Updates - D - Feature Update - Broad Ring - v1.0 26

12.1.2. Win - Updates - D - Feature Update - Pilot Ring - v1.0 27

12.1.3. Win - Updates - D - Feature Update - Preview Ring - v1.0 27

13. Device compliance 28

13.1. Compliance Policies 28

13.1.1. Win - Compliance - Default - C - Broad v1.0.0 28

13.1.2. Win - Compliance - U - Defender for Endpoint - v1.0.0 30

13.1.3. Win - Compliance - U - Device Health - v1.0.0 32

13.1.4. Win - Compliance - U - Device Security - v1.0.0 34

13.1.5. Win - Compliance - U - Password - v1.0.0 36

14. Windows enrollment 38

14.1. Autopilot 38

14.1.1. StAH Shared Device Entra ID Joined Self Deploying 38

14.1.2. StAH Standard Device Entra ID Joined 39

14.2. Enrollment Status Page 40

14.2.1. All users and all devices 40

14.2.2. StAH Standard Device Entra ID Joined 41

14.2.3. StAH Standard Device Entra ID Joined - UAT 42

15. Driver updates for Windows 10 and later 43

15.1. Driver Update Profiles 43

15.1.1. Win - Updates - U - Driver Update - Broad Ring - v1.0 43

15.1.2. Win - Updates - U - Driver Update - Pilot Ring - v1.0 44

15.1.3. Win - Updates - U - Driver Update - Preview Ring - v1.0 44

16. Device configuration 45

16.1. Settings Catalog 45

16.1.1. Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules 45

16.1.2. \*\*Win - Device Security - U - Windows Spotlight and Org Messages - v1.0.0 46

16.1.3. \*\*Win - Encryption - U - Personal Data Encryption - v1.0.0 46

16.1.4. \*\*Win - Microsoft Edge - D - Enterprise Mode Cloud Site List - v1.0.0 47

16.1.5. \*\*Win - Windows Hello for Business - D - Cloud Kerberos Trust - v1.0.0 48

16.1.6. \*\*Win - Windows Hello for Business - D - Configuration - v1.0.0 48

16.1.7. \*\*X - Win - Dispensation - CIS -L1 - Bitlocker - D - v1.0.0 49

16.1.8. \*\*X - Win - Dispensation - CIS -L2 - D - v1.0.0 50

16.1.9. \*Win - Windows LAPS - D - LAPS Configuration - v1.0.0 50

16.1.10. Win - CIS - Level 2 - Admin Templates - D - v3.0.1 51

16.1.11. Win - CIS - Level 2 - No Services - D - v3.0.1 54

16.1.12. Win - Defender Antivirus - D - Configuration - v1.0.0 55

16.1.13. Win - Defender Antivirus - D - Security Experience - v1.0.0 56

16.1.14. Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0 57

16.1.15. Win - Defender Attack Surface Reduction - D - ASR Rules (Block Mode) - v1.0.0 59

16.1.16. Win - Device Security - D - Audit and Event Logging - v1.0.0 60

16.1.17. Win - Device Security - D - Config Refresh - v1.0.0 62

16.1.18. Win - Device Security - D - Enhanced Phishing Protection - v1.0.0 63

16.1.19. Win - Device Security - D - Local Security Policies - v1.0.0 63

16.1.20. Win - Device Security - D - Location and Privacy - v1.0.0 65

16.1.21. Win - Device Security - D - Login and Lock Screen - v1.0.0 66

16.1.22. Win - Device Security - D - Network List Manager - v1.0.0 67

16.1.23. Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0 68

16.1.24. Win - Device Security - D - Security Hardening - v1.0.0 69

16.1.25. Win - Device Security - D - Timezone - v1.0.0 73

16.1.26. Win - Device Security - D - User Rights - v1.0.0 74

16.1.27. Win - Device Security - D - Windows Package Manager - v1.0.0 75

16.1.28. Win - Device Security - D - Windows Subsystem for Linux - v1.0.0 75

16.1.29. Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0 76

16.1.30. Win - Device Security - U - Power and Device Lock - v1.0.0 77

16.1.31. Win - Device Security - U - Windows Sandbox - v1.0.0 79

16.1.32. Win - Dispensation - CIS -L1 - D - v1.0.0 79

16.1.33. Win - Dispensation - CIS -L1 - U - v1.0.0 80

16.1.34. Win - Encryption - D - BitLocker (OS Disk) - v1.0.0 81

16.1.35. Win - Health Monitoring - D - MDM wins over GPO - v1.0.0 83

16.1.36. Win - Health Monitoring - D - Windows Update for Business - v1.0.0 83

16.1.37. Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0 84

16.1.38. Win - Internet Explorer (Legacy) - D - Security - v1.0.0 85

16.1.39. Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0 93

16.1.40. Win - MDE - D - Onboarding - v1.0.0 96

16.1.41. Win - Microsoft Accounts - D - Configuration - v1.0.0 97

16.1.42. Win - Microsoft Edge - D - Security - v1.0.0 98

16.1.43. Win - Microsoft Edge - U - Extensions - v1.1.0 103

16.1.44. Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0 106

16.1.45. Win - Microsoft Edge - U - Password Management - v1.0.0 110

16.1.46. Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0 110

16.1.47. Win - Microsoft Edge - U - User Experience - v1.0.0 111

16.1.48. Win - Microsoft Office - U - Config and Experience - v1.0.0 113

16.1.49. Win - Microsoft Office - U - Macros - ALLOW - v1.0.0 115

16.1.50. Win - Microsoft Office - U - Macros - BLOCK - v1.0.0 116

16.1.51. Win - Microsoft OneDrive - D - Configuration - v1.0.0 117

16.1.52. Win - Microsoft OneDrive - U - Configuration - v1.0.0 120

16.1.53. Win - Microsoft Store - D - Configuration - v1.0.0 121

16.1.54. Win - Microsoft Store - U - Configuration - v1.0.0 121

16.1.55. Win - Updates - D - Microsoft Edge - v1.0.0 122

16.1.56. Win - Updates - D - Microsoft Office - v1.0.0 124

16.1.57. Win - Updates - D - WUfB Delivery Optimisation - v1.0.0 124

16.1.58. Win - Updates - D - WUfB Restart Warnings - v1.0.0 125

16.1.59. Win - Updates - U - Defender Updates - Broad - v1.0.0 126

16.1.60. Win - Updates - U - Defender Updates - Pilot - v1.0.0 127

16.1.61. Win - Updates - U - Defender Updates - Preview - v1.0.0 127

16.1.62. Win - Updates - U - Microsoft Office - Broad - v1.0.0 128

16.1.63. Win - Updates - U - Microsoft Office - Pilot - v1.0.0 129

16.1.64. Win - Updates - U - Microsoft Office - Preview - v1.0.0 130

16.1.65. Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0 130

16.1.66. Win - Updates - U - Microsoft OneDrive - Pilot - v1.0.0 131

16.1.67. Win - Updates - U - Microsoft OneDrive - Preview - v1.0.0 131

16.1.68. Win - USB Device Control - D - Device Control - v1.0.0 Device Control 132

16.1.69. Win - User Experience - D - Background and Lockscreen - v2.0.0 133

16.1.70. Win - User Experience - D - Feature Configuration - v1.0.0 134

16.1.71. Win - User Experience - D - Storage Sense - v1.0.0 135

16.1.72. Win - User Experience - U - Start Menu - v1.0.0 136

16.1.73. Win - Windows Firewall - D - Firewall Configuration - v1.0.0 137

16.1.74. Win - Windows Hello for Business - D - Disable Configuration - v1.0.0 139

16.1.75. Win - Windows LAPS - D - LAPS Configuration - v1.0.1 139

16.2. Templates 140

16.2.1. \*\*Win - Application Control - D - AppLocker - BLOCK - v1.0.0 140

16.2.2. \*\*Win - User Experience - D - Background and Lockscreen - v1.0.0 154

16.2.3. Win - Application Control - D - AppLocker - AUDIT - v1.0.0 158

16.2.4. Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0 172

16.2.5. Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0 172

16.2.6. Win - Certificate - D - St Andrews Device Cert - v2.0.0 173

16.2.7. Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0 174

16.2.8. Win - Certificate - D - St Andrews Root Cert - v1.0.0 175

16.2.9. Win - Certificate - U - St Andrews User Cert - v1.0.0 175

16.2.10. Win - Health Monitoring - D - Endpoint Analytics - v1.0.0 176

16.2.11. Win - Shared Multi User Device - D - TBA- v1.0.0 177

16.2.12. Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0 177

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes | Author |
| D01 |  | Initial Draft | Nic Fuller |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Revision History

#### Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Date | Signature |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Introduction

St Andrew’s Healthcare is enhancing its endpoint management and operational efficiency through the implementation of Microsoft Endpoint Manager (MEM), incorporating a comprehensive suite of configurations designed to align with industry best practices. This document provides a formal outline of the design and rationale for the Open Intune Baseline, offering a structured approach to device management across the organization’s Windows 10 and Windows 11 estate.

The Open Intune Baseline serves as a foundational framework that standardizes device configurations, ensuring consistent application of policies for updates, compliance, and device security. By leveraging MEM’s advanced capabilities, St Andrew’s Healthcare can streamline the deployment and management of Windows devices, ensuring that they remain compliant with organizational policies and optimally configured for performance and reliability.

The document details key configurations such as update rings, device compliance policies, feature updates, driver management, and device configuration settings. It also covers enrolment methods, including Autopilot profiles, which enable seamless and automated onboarding of new devices with minimal administrative overhead. The use of targeted filters ensures that policies are applied precisely to the appropriate device groups, enhancing both security and user experience without unnecessary complexity.

In summary, this documentation demonstrates St Andrew’s Healthcare’s commitment to leveraging Microsoft Endpoint Manager and the Open Intune Baseline to achieve operational excellence, ensuring consistent device configurations, minimizing management overhead, and enabling a scalable and resilient endpoint management strategy.

1. St Andrews Intune Configuration
   1. Filters

The Filters section serves as a critical mechanism for precisely targeting policies and configurations to specific devices within the Microsoft Intune environment at St Andrew’s Healthcare. Filters leverage GroupTags and enrolment profile names to include or exclude devices dynamically based on their attributes or deployment status. This capability is essential for managing diverse device populations, including standard and shared-use devices, each requiring distinct policies.

The StAH-Win-Filter-Baseline - All GroupTags filter encompasses all devices tagged as either standard or shared, ensuring comprehensive coverage for baseline configurations. It uses logical conditions to include devices with enrollment profiles like StAH Standard Device Entra ID Joined and StAH Shared Device Entra ID Joined Self Deploying.

The StAH-Win-Filter-Shared-GroupTag narrows the focus to shared devices only, ensuring that policies specific to multi-user environments are applied accurately.

Similarly, the StAH-Win-Filter-Standard GroupTag targets standard devices, applying individual user configurations while excluding shared-use devices.

By combining these filters, administrators can granularly control policy assignments, ensuring that each device receives appropriate configurations based on its role and deployment profile. This level of targeting helps enforce security, compliance, and user experience policies tailored to the needs of specific device groups, while also supporting efficient management across a large and varied device estate.

* + 1. \*StAH-Win-Filter-Shared-GroupTag

1. Update rings for Windows 10 and later

The Update rings section outlines the strategies and configurations for managing Windows update deployment within St Andrew’s Healthcare. This includes policies for broad, pilot, and preview rings, providing controlled rollout paths for quality and feature updates. By organizing devices into rings, IT administrators can test updates on a subset of devices before deploying them organization-wide, ensuring stability and minimizing disruption.

* 1. Update Policies

1. Scripts

The Scripts section introduces the custom PowerShell scripts used to automate system configuration and management within St Andrew’s Healthcare’s Intune environment. These scripts streamline processes such as application removal and service configuration, reducing manual effort and increasing operational efficiency. They play a critical role in enforcing security baselines and maintaining system integrity across enrolled devices.

* 1. Scripts (PowerShell)

This section contains PowerShell scripts used to automate tasks such as application removal and configuration, simplifying system management.

1. Feature updates for Windows 10 and later

The Feature updates section manages the deployment of new Windows 10 and Windows 11 features, ensuring that devices receive timely updates aligned with organizational requirements. This section provides structured rollout configurations for feature updates, balancing the introduction of new capabilities with system stability and compliance.

* 1. Feature Updates

Feature Updates defines how major Windows version upgrades are managed and rolled out, ensuring that devices are kept current with new features and improvements.

1. Device compliance

The Device compliance section establishes policies that ensure devices meet the security and health standards of St Andrew’s Healthcare. By enforcing requirements such as encryption, password policies, and Defender configurations, this section safeguards sensitive data and minimizes potential vulnerabilities across managed endpoints.

1. Windows enrollment

The Windows enrollment section details the configuration of Autopilot profiles and enrollment settings, streamlining the deployment and provisioning of Windows devices. Through self-deploying and user-driven modes, St Andrew’s Healthcare ensures a seamless onboarding experience for both shared and standard devices, with predefined configurations applied automatically.

* 1. Autopilot

The Autopilot section outlines the deployment profiles and configurations that automate the enrollment and setup of Windows devices. These profiles help streamline device provisioning and ensure compliance with organizational policies.

* + 1. StAH Shared Device Entra ID Joined Self Deploying

This Autopilot profile configures shared devices for self-deployment, minimizing manual setup and maintaining security.

1. Driver updates for Windows 10 and later

The Driver updates section defines the approval and deployment strategies for device drivers in the organization. By categorizing driver updates into broad, pilot, and preview rings, this section helps balance the need for hardware compatibility with the importance of system reliability and performance.

* 1. Templates

The Templates section provides pre-defined configurations and AppLocker rules for applications, certificates, and trusted content. By leveraging these templates, St Andrew’s Healthcare can quickly apply consistent settings across devices, enhancing both security and productivity while maintaining compliance with organizational policies.

1. Tenant admin
   1. Filters
      1. \*StAH-Win-Filter-Baseline - All

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*StAH-Win-Filter-Baseline - All |
| Description |  |
| Created | 23 July 2025 10:20:08 |
| Last modified | 23 July 2025 10:20:09 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 1. Basics - \*StAH-Win-Filter-Baseline - All

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.enrollmentProfileName -eq "StAH Standard Device Entra ID Joined") or (device.enrollmentProfileName -eq "StAH Shared Device Entra ID Joined Self Deploying") or (device.deviceName -eq "W10-CHSH2R2") or (device.deviceName -eq "W10-7HZWRQ2") or (device.deviceName -eq "W10-24VX5Q2") or (device.deviceName -eq "W10-60RF0Z2") or (device.deviceName -eq "W10-J9Q11F3") or (device.deviceName -eq "W10-58ZK5S2") or (device.deviceName -eq "W10-DCZ21F3") or (device.deviceName -eq "W10-DWTR2D3") or (device.deviceName -eq "W10-4VM3MQ2") or (device.deviceName -eq "W10-2LQNNV2") or (device.deviceName -eq "W10-F9TF6S2") or (device.deviceName -eq "W10-48HDVT2") or (device.deviceName -eq "W10-JLV5273") or (device.deviceName -eq "W10-FF3C5Q2") or (device.deviceName -eq "W10-9MB45S2") or (device.deviceName -eq "W10-DLTK0X2") or (device.deviceName -eq "W10-93YS5S2") or (device.deviceName -eq "W10-78642N2") or (device.deviceName -eq "W10-3Z5C0X2") or (device.deviceName -eq "W10-DT1K5S2") or (device.deviceName -eq "W10-CV7LST3") |

Table 2. Settings - \*StAH-Win-Filter-Baseline - All

* + 1. \*StAH-Win-Filter-Baseline - All GroupTags

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*StAH-Win-Filter-Baseline - All GroupTags |
| Description | This will filter on devices with the Autopilot GroupTag of "StAH-STD" and which have therefore run the following deployment profile: "StAH Standard Device Entra ID Joined" or the GroupTag of "StAH-Shared" which have run the follwing deployment profile "StAH Shared Device Entra ID Joined Self Deploying" |
| Created | 09 June 2025 14:40:42 |
| Last modified | 09 June 2025 14:40:42 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 3. Basics - \*StAH-Win-Filter-Baseline - All GroupTags

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.enrollmentProfileName -eq "StAH Standard Device Entra ID Joined") or (device.enrollmentProfileName -eq "StAH Shared Device Entra ID Joined Self Deploying") |

Table 4. Settings - \*StAH-Win-Filter-Baseline - All GroupTags

* + 1. \*StAH-Win-Filter-Shared-GroupTag

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*StAH-Win-Filter-Shared-GroupTag |
| Description |  |
| Created | 15 April 2025 15:14:51 |
| Last modified | 15 April 2025 15:14:51 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 5. Basics - \*StAH-Win-Filter-Shared-GroupTag

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.enrollmentProfileName -eq "StAH Shared Device Entra ID Joined Self Deploying") |

Table 6. Settings - \*StAH-Win-Filter-Shared-GroupTag

* + 1. \*StAH-Win-Filter-Standard GroupTag

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*StAH-Win-Filter-Standard GroupTag |
| Description |  |
| Created | 15 April 2025 15:21:53 |
| Last modified | 15 April 2025 15:21:53 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 7. Basics - \*StAH-Win-Filter-Standard GroupTag

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.enrollmentProfileName -eq "StAH Standard Device Entra ID Joined") |

Table 8. Settings - \*StAH-Win-Filter-Standard GroupTag

* + 1. StAH-Win-Filter-EntraID Hybrid Joined

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH-Win-Filter-EntraID Hybrid Joined |
| Description | This filter will include all devices that are EntraID Hybrid Joined |
| Created | 10 April 2025 09:22:50 |
| Last modified | 10 April 2025 09:22:50 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 9. Basics - StAH-Win-Filter-EntraID Hybrid Joined

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.deviceTrustType -eq "Hybrid Azure AD joined") |

Table 10. Settings - StAH-Win-Filter-EntraID Hybrid Joined

* + 1. StAH-Win-Filter-EntraID Joined

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH-Win-Filter-EntraID Joined |
| Description | This filter will include all devices that are EntraID Joined |
| Created | 10 April 2025 09:22:50 |
| Last modified | 10 April 2025 09:22:50 |
| Profile type | Filters |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 11. Basics - StAH-Win-Filter-EntraID Joined

|  |  |
| --- | --- |
| Name | Value |
| Rules | |
| Rule syntax | (device.deviceTrustType -eq "Azure AD joined") |

Table 12. Settings - StAH-Win-Filter-EntraID Joined

1. Update rings for Windows 10 and later
   1. Update Policies
      1. Win - Updates - U - Update Ring - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Update Ring - Broad Ring - v1.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Software Updates |
| Created | 21 March 2025 09:03:55 |
| Last modified | 17 June 2025 10:10:42 |
| Version | 2 |
| Scope tags | Default |

Table 13. Basics - Win - Updates - U - Update Ring - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Update settings | |
| Windows drivers | Allow |
| Quality update deferral period (days) | 8 |
| Feature update deferral period (days) | 0 |
| Upgrade Windows 10 devices to Latest Windows 11 release | No |
| Set feature update uninstall period (2 - 60 days) | 30 |
| User experience settings | |
| Automatic update behavior | Reset to default |
| Restart checks (EDU Restart) | Allow |
| Option to pause Windows updates | Disable |
| Use deadline settings | Allow |
| Deadline for feature updates | 1 |
| Deadline for quality updates | 1 |
| Grace period | 1 |
| Auto reboot before deadline | No |

Table 14. Settings - Win - Updates - U - Update Ring - Broad Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |
| Excluded Groups | | |
| Intune-Update-Preview-UAT |  |  |
| Intune-Updates-Preview-Devices |  |  |

Table 15. Assignments - Win - Updates - U - Update Ring - Broad Ring - v1.0

* + 1. Win - Updates - U - Update Ring - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Update Ring - Pilot Ring - v1.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Software Updates |
| Created | 21 March 2025 09:03:55 |
| Last modified | 17 June 2025 10:10:21 |
| Version | 2 |
| Scope tags | Default |

Table 16. Basics - Win - Updates - U - Update Ring - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Update settings | |
| Windows drivers | Allow |
| Quality update deferral period (days) | 3 |
| Feature update deferral period (days) | 0 |
| Upgrade Windows 10 devices to Latest Windows 11 release | No |
| Set feature update uninstall period (2 - 60 days) | 30 |
| User experience settings | |
| Automatic update behavior | Reset to default |
| Restart checks (EDU Restart) | Allow |
| Option to pause Windows updates | Disable |
| Use deadline settings | Allow |
| Deadline for feature updates | 1 |
| Deadline for quality updates | 1 |
| Grace period | 1 |
| Auto reboot before deadline | No |

Table 17. Settings - Win - Updates - U - Update Ring - Pilot Ring - v1.0

* + 1. Win - Updates - U - Update Ring - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Update Ring - Preview Ring - v1.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Software Updates |
| Created | 21 March 2025 09:03:55 |
| Last modified | 17 June 2025 10:10:02 |
| Version | 3 |
| Scope tags | Default |

Table 18. Basics - Win - Updates - U - Update Ring - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Update settings | |
| Windows drivers | Allow |
| Quality update deferral period (days) | 1 |
| Feature update deferral period (days) | 0 |
| Upgrade Windows 10 devices to Latest Windows 11 release | No |
| Set feature update uninstall period (2 - 60 days) | 30 |
| User experience settings | |
| Automatic update behavior | Reset to default |
| Restart checks (EDU Restart) | Allow |
| Option to pause Windows updates | Disable |
| Use deadline settings | Allow |
| Deadline for feature updates | 1 |
| Deadline for quality updates | 1 |
| Grace period | 1 |
| Auto reboot before deadline | No |

Table 19. Settings - Win - Updates - U - Update Ring - Preview Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Update-Preview-UAT | None | None |
| Intune-Updates-Preview-Devices | None | None |

Table 20. Assignments - Win - Updates - U - Update Ring - Preview Ring - v1.0

1. Scripts
   1. Scripts (PowerShell)
      1. Remove-Bloatware

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Remove-Bloatware |
| Description |  |
| Profile type | PowerShell script |
| Created | 12 May 2025 14:02:53 |
| Last modified | 02 July 2025 11:42:52 |
| Scope tags | Default |

Table 21. Basics - Remove-Bloatware

|  |  |
| --- | --- |
| Name | Value |
| Script settings | |
| PowerShell script | Remove-Bloatware.ps1 |
| Run this script using the logged on credentials | No |
| Enforce script signature check | No |
| Run script in 64 bit PowerShell Host | No |

Table 22. Settings - Remove-Bloatware

|  |
| --- |
| Remove-Bloatware.ps1 |
| ﻿<#  .SYNOPSIS  Remove built-in apps (modern apps) from Windows 10.  .DESCRIPTION  This script will remove all built-in apps with a provisioning package that's not specified in the 'white-list' in this script.  It supports MDT and ConfigMgr usage, but only for online scenarios, meaning it can't be executed during the WinPE phase.  For a more detailed list of applications available in each version of Windows 10, refer to the documentation here:  https://docs.microsoft.com/en-us/windows/application-management/apps-in-windows-10  .EXAMPLE  .\Invoke-RemoveBuiltinApps.ps1  .NOTES  FileName: Invoke-RemoveBuiltinApps.ps1  Author: Nickolaj Andersen  Contact: @NickolajA  Created: 2019-03-10  Updated: 2021-02-02  Version history:  1.0.0 - (2019-03-10) Initial script updated with help section and a fix for randomly freezing  1.1.0 - (2019-05-03) Added support for Windows 10 version 1903 (19H1)  1.1.1 - (2019-08-13) Removed the part where it was disabling/enabling configuration for Store updates, as it's not needed  1.1.2 - (2019-10-03) Removed unnecessary left over functions and updated catch statements so that they actually log the current app that could not be removed  1.2.0 - (2021-02-02) Added support for Windows 10 version 2004 (20H1) and 20H2  #>  Begin {  # White list of Features On Demand V2 packages  $WhiteListOnDemand = "NetFX3|DirectX|Tools.DeveloperMode.Core|Language|InternetExplorer|ContactSupport|OneCoreUAP|WindowsMediaPlayer|Hello.Face|Notepad|MSPaint|PowerShell.ISE|ShellComponents"  # White list of appx packages to keep installed  $WhiteListedApps = New-Object -TypeName System.Collections.ArrayList  $WhiteListedApps.AddRange(@(  "Microsoft.DesktopAppInstaller",  # "Microsoft.Office.OneNote",  "Microsoft.Messaging",  "Microsoft.MSPaint",  "Microsoft.Windows.Photos",  "Microsoft.StorePurchaseApp",  # "Microsoft.MicrosoftOfficeHub",  "Microsoft.MicrosoftStickyNotes",  "Microsoft.WindowsAlarms",  "Microsoft.WindowsCalculator",  # "Microsoft.WindowsCommunicationsApps", # Mail, Calendar etc  "Microsoft.WindowsSoundRecorder",  "Microsoft.WindowsStore"  ))  # Windows 10 version 1809  $WhiteListedApps.AddRange(@(  "Microsoft.ScreenSketch",  "Microsoft.HEIFImageExtension",  "Microsoft.VP9VideoExtensions",  "Microsoft.WebMediaExtensions",  "Microsoft.WebpImageExtension"  ))  # Windows 10 version 1903  # No new apps  # Windows 10 version 1909  $WhiteListedApps.AddRange(@(  "Microsoft.Outlook.DesktopIntegrationServicess"  ))  # Windows 10 version 2004  $WhiteListedApps.AddRange(@(  "Microsoft.VCLibs.140.00"  ))  # Windows 10 version 20H2  $WhiteListedApps.AddRange(@(  "Microsoft.MicrosoftEdge.Stable"  ))  }  Process {  # Functions  function Write-LogEntry {  param(  [parameter(Mandatory=$true, HelpMessage="Value added to the RemovedApps.log file.")]  [ValidateNotNullOrEmpty()]  [string]$Value,  [parameter(Mandatory=$false, HelpMessage="Name of the log file that the entry will written to.")]  [ValidateNotNullOrEmpty()]  [string]$FileName = "RemovedApps.log"  )  # Determine log file location  $LogFilePath = Join-Path -Path $env:windir -ChildPath "Temp\$($FileName)"  # Add value to log file  try {  Out-File -InputObject $Value -Append -NoClobber -Encoding Default -FilePath $LogFilePath -ErrorAction Stop  }  catch [System.Exception] {  Write-Warning -Message "Unable to append log entry to $($FileName) file"  }  }  # Initial logging  Write-LogEntry -Value "Starting built-in AppxPackage, AppxProvisioningPackage and Feature on Demand V2 removal process"  # Determine provisioned apps  $AppArrayList = Get-AppxProvisionedPackage -Online | Select-Object -ExpandProperty DisplayName  # Loop through the list of appx packages  foreach ($App in $AppArrayList) {  Write-LogEntry -Value "Processing appx package: $($App)"  # If application name not in appx package white list, remove AppxPackage and AppxProvisioningPackage  if (($App -in $WhiteListedApps)) {  Write-LogEntry -Value "Skipping excluded application package: $($App)"  }  else {  # Gather package names  $AppPackageFullName = Get-AppxPackage -Name $App | Select-Object -ExpandProperty PackageFullName -First 1  $AppProvisioningPackageName = Get-AppxProvisionedPackage -Online | Where-Object { $\_.DisplayName -like $App } | Select-Object -ExpandProperty PackageName -First 1  # Attempt to remove AppxPackage  if ($AppPackageFullName -ne $null) {  try {  Write-LogEntry -Value "Removing AppxPackage: $($AppPackageFullName)"  Remove-AppxPackage -Package $AppPackageFullName -ErrorAction Stop | Out-Null  }  catch [System.Exception] {  Write-LogEntry -Value "Removing AppxPackage '$($AppPackageFullName)' failed: $($\_.Exception.Message)"  }  }  else {  Write-LogEntry -Value "Unable to locate AppxPackage for current app: $($App)"  }  # Attempt to remove AppxProvisioningPackage  if ($AppProvisioningPackageName -ne $null) {  try {  Write-LogEntry -Value "Removing AppxProvisioningPackage: $($AppProvisioningPackageName)"  Remove-AppxProvisionedPackage -PackageName $AppProvisioningPackageName -Online -ErrorAction Stop | Out-Null  }  catch [System.Exception] {  Write-LogEntry -Value "Removing AppxProvisioningPackage '$($AppProvisioningPackageName)' failed: $($\_.Exception.Message)"  }  }  else {  Write-LogEntry -Value "Unable to locate AppxProvisioningPackage for current app: $($App)"  }  }  }  Write-LogEntry -Value "Starting Features on Demand V2 removal process"  # Get Features On Demand that should be removed  try {  $OSBuildNumber = Get-WmiObject -Class "Win32\_OperatingSystem" | Select-Object -ExpandProperty BuildNumber  # Handle cmdlet limitations for older OS builds  if ($OSBuildNumber -le "16299") {  $OnDemandFeatures = Get-WindowsCapability -Online -ErrorAction Stop | Where-Object { $\_.Name -notmatch $WhiteListOnDemand -and $\_.State -like "Installed" } | Select-Object -ExpandProperty Name  }  else {  $OnDemandFeatures = Get-WindowsCapability -Online -LimitAccess -ErrorAction Stop | Where-Object { $\_.Name -notmatch $WhiteListOnDemand -and $\_.State -like "Installed" } | Select-Object -ExpandProperty Name  }  foreach ($Feature in $OnDemandFeatures) {  try {  Write-LogEntry -Value "Removing Feature on Demand V2 package: $($Feature)"  # Handle cmdlet limitations for older OS builds  if ($OSBuildNumber -le "16299") {  Get-WindowsCapability -Online -ErrorAction Stop | Where-Object { $\_.Name -like $Feature } | Remove-WindowsCapability -Online -ErrorAction Stop | Out-Null  }  else {  Get-WindowsCapability -Online -LimitAccess -ErrorAction Stop | Where-Object { $\_.Name -like $Feature } | Remove-WindowsCapability -Online -ErrorAction Stop | Out-Null  }  }  catch [System.Exception] {  Write-LogEntry -Value "Removing Feature on Demand V2 package failed: $($\_.Exception.Message)"  }  }  }  catch [System.Exception] {  Write-LogEntry -Value "Attempting to list Feature on Demand V2 packages failed: $($\_.Exception.Message)"  }  # Complete  Write-LogEntry -Value "Completed built-in AppxPackage, AppxProvisioningPackage and Feature on Demand V2 removal process"  EXIT 0  $host.exit  } |

Table 23. PowerShell script - Remove-Bloatware

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Windows11-PoC-User | None | None |
| Intune-Test-SecurityPolicies-Device | None | None |

Table 24. Assignments - Remove-Bloatware

* + 1. Windows 11 v3.0.1 Services CIS L2

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Windows 11 v3.0.1 Services CIS L2 |
| Description | This script will disable the following services:  "BTAGService", # Bluetooth Audio Gateway Service  "bthserv", # Bluetooth Support Service  "MapsBroker", # Downloaded Maps Manager  "lfsvc", # Geolocation Service  "lltdsvc", # Link-Layer Topology Discovery Mapper  "MSiSCSI", # Microsoft iSCSI Initiator Service  "PNRPsvc", # Peer Name Resolution Protocol  "p2psvc", # Peer Networking Grouping  "p2pimsvc", # Peer Networking Identity Manager  "PNRPAutoReg", # PNRP Machine Name Publication Service  "wercplsupport", # Problem Reports and Solutions Control Panel Support  "RasAuto", # Remote Access Auto Connection Manager  "SessionEnv", # Remote Desktop Configuration  "TermService", # Remote Desktop LocalServices  "UmRdpService", # Remote Desktop LocalServices UserMode Port Redirector  "RemoteRegistry", # Remote Registry  "LanmanServer", # Server  "SNMP", # SNMP Service  "WerSvc", # Windows Error Reporting Service  "Wecsvc", # Windows Event Collector  "WpnService", # Windows Push Notifications System Service  "PushToInstall", # Windows PushToInstall Service  "WinRM" # Windows Remote Management |
| Profile type | PowerShell script |
| Created | 10 April 2025 09:26:50 |
| Last modified | 23 April 2025 12:03:10 |
| Scope tags | Default |

Table 25. Basics - Windows 11 v3.0.1 Services CIS L2

|  |  |
| --- | --- |
| Name | Value |
| Script settings | |
| PowerShell script | Windows 11 v3.0.1 Services L2 - No Spooler.ps1 |
| Run this script using the logged on credentials | No |
| Enforce script signature check | No |
| Run script in 64 bit PowerShell Host | No |

Table 26. Settings - Windows 11 v3.0.1 Services CIS L2

|  |
| --- |
| Windows 11 v3.0.1 Services L2 - No Spooler.ps1 |
| <##############################################################################    CIS Microsoft Intune for Windows 11 Benchmark v3.0.1 Build Kit script  Section #69 - System Services  Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)  The purpose of this script is to configure a system using the recommendations  provided in the Benchmark, section(s), and profile level listed above to a  hardened state consistent with a CIS Benchmark.    The script can be tailored to the organization's needs such as by creating  exceptions or adding additional event logging.  This script can be deployed through various means, including Intune script  manager, running it locally, or through any automation tool.  Version: 1.0  Updated: 12.Feb.2024 by ceifert  ##############################################################################>  #Requires -RunAsAdministrator  $L2Services = @(  "BTAGService", # Bluetooth Audio Gateway Service  "bthserv", # Bluetooth Support Service  "MapsBroker", # Downloaded Maps Manager  "lfsvc", # Geolocation Service  "lltdsvc", # Link-Layer Topology Discovery Mapper  "MSiSCSI", # Microsoft iSCSI Initiator Service  "PNRPsvc", # Peer Name Resolution Protocol  "p2psvc", # Peer Networking Grouping  "p2pimsvc", # Peer Networking Identity Manager  "PNRPAutoReg", # PNRP Machine Name Publication Service  "wercplsupport", # Problem Reports and Solutions Control Panel Support  "RasAuto", # Remote Access Auto Connection Manager  "SessionEnv", # Remote Desktop Configuration  "TermService", # Remote Desktop LocalServices  "UmRdpService", # Remote Desktop LocalServices UserMode Port Redirector  "RemoteRegistry", # Remote Registry  "LanmanServer", # Server  "SNMP", # SNMP Service  "WerSvc", # Windows Error Reporting Service  "Wecsvc", # Windows Event Collector  "WpnService", # Windows Push Notifications System Service  "PushToInstall", # Windows PushToInstall Service  "WinRM" # Windows Remote Management  )  # Get current state on the services in the array above.  $LocalServices = Get-Service -Name $L2Services -ErrorAction SilentlyContinue  $DisabledCount = 0  $AlreadyDisabledCount = 0  $NotInstalledCount = 0  foreach ($service in $L2Services) {  # Make sure service name in the list matches with local system services.  # Added because of Computer Browser mismatch with "bowser" service  $FoundService = $LocalServices | Where-Object { $\_.Name -eq $service }  if ($FoundService) {  if ($FoundService.StartType -ne 'Disabled') {  Set-Service $FoundService.Name -StartupType Disabled -Verbose  $DisabledCount++  } else {  Write-Host "Service $($FoundService.DisplayName) is already disabled." -ForegroundColor Green  $AlreadyDisabledCount++  }  } else {  Write-Host "Service $service not installed." -ForegroundColor Green  $NotInstalledCount++  }  }  Write-Host "`nThis script configured $DisabledCount services as 'Disabled'." -ForegroundColor Cyan  Write-Host "$AlreadyDisabledCount services were already disabled and $NotInstalledCount are not installed." -ForegroundColor Green |

Table 27. PowerShell script - Windows 11 v3.0.1 Services CIS L2

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Dynamic Group-Standard Entra ID Device | None | None |
| StAH-Dynamic Group-Shared Entra ID Device | None | None |

Table 28. Assignments - Windows 11 v3.0.1 Services CIS L2

1. Feature updates for Windows 10 and later
   1. Feature Updates
      1. Win - Updates - D - Feature Update - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - Feature Update - Broad Ring - v1.0 |
| Description |  |
| Policy type | Feature updates for Windows 10 and later |
| Created | 21 March 2025 09:02:21 |
| Last modified | 17 June 2025 10:11:00 |
| Scope tags | Default |

Table 29. Basics - Win - Updates - D - Feature Update - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Deployment settings | |
| Feature update to deploy | Windows 10, version 22H2 |
| Required or optional update | Make available to users as a required update |
| When a device isn't eligible to run Windows 11, install the latest Windows 10 feature update | No |
| Rollout options | Make update available as soon as possible |

Table 30. Settings - Win - Updates - D - Feature Update - Broad Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Default-Broad-Devices | None | None |
| Excluded Groups | | |
| Intune-Update-Preview-UAT |  |  |
| Intune-Updates-Preview-Devices |  |  |

Table 31. Assignments - Win - Updates - D - Feature Update - Broad Ring - v1.0

* + 1. Win - Updates - D - Feature Update - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - Feature Update - Pilot Ring - v1.0 |
| Description |  |
| Policy type | Feature updates for Windows 10 and later |
| Created | 21 March 2025 09:02:21 |
| Last modified | 29 May 2025 16:07:41 |
| Scope tags | Default |

Table 32. Basics - Win - Updates - D - Feature Update - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Deployment settings | |
| Feature update to deploy | Windows 11, version 23H2 |
| Required or optional update | Make available to users as a required update |
| When a device isn't eligible to run Windows 11, install the latest Windows 10 feature update | No |
| Rollout options | Make update available as soon as possible |

Table 33. Settings - Win - Updates - D - Feature Update - Pilot Ring - v1.0

* + 1. Win - Updates - D - Feature Update - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - Feature Update - Preview Ring - v1.0 |
| Description |  |
| Policy type | Feature updates for Windows 10 and later |
| Created | 21 March 2025 09:02:21 |
| Last modified | 29 May 2025 16:07:10 |
| Scope tags | Default |

Table 34. Basics - Win - Updates - D - Feature Update - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Deployment settings | |
| Feature update to deploy | Windows 11, version 23H2 |
| Required or optional update | Make available to users as a required update |
| When a device isn't eligible to run Windows 11, install the latest Windows 10 feature update | No |
| Rollout options | Make update available as soon as possible |

Table 35. Settings - Win - Updates - D - Feature Update - Preview Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Dynamic Group-Standard Entra ID Device | None | None |
| StAH-Dynamic Group-Shared Entra ID Device | None | None |
| Intune-Update-Preview-UAT | None | None |
| Intune-Updates-Preview-Devices | None | None |

Table 36. Assignments - Win - Updates - D - Feature Update - Preview Ring - v1.0

1. Device compliance
   1. Compliance Policies
      1. Win - Compliance - Default - C - Broad v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Compliance - Default - C - Broad v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Windows 10 and later compliance policy |
| Created | 03 March 2025 15:44:19 |
| Last modified | 03 March 2025 15:44:19 |
| Version | 1 |
| Scope tags | Default |

Table 37. Basics - Win - Compliance - Default - C - Broad v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Custom Compliance | |
| Custom compliance | Not configured |
| Device Health | |
| Windows 10 and 11 | |
| BitLocker | Not configured |
| Secure Boot | Not configured |
| Code integrity | Not configured |
| Windows 11 only | |
| Early Launch AntiMalware | Not configured |
| Firmware Protection | Not configured |
| Memory Integrity Protection | Not configured |
| Memory Access Protection | Not configured |
| Virtualization-based Security | Not configured |
| Device Properties | |
| Operating System Version | |
| Minimum OS version | 10.0.19045.0 |
| Maximum OS version |  |
| Minimum OS version for mobile devices |  |
| Maximum OS version for mobile devices |  |
| Valid operating system builds |  |
| Configuration Manager Compliance | |
| Require device compliance from Configuration Manager | Not configured |
| System Security | |
| Password | |
| Require a password to unlock mobile devices | Not configured |
| Simple passwords | Not configured |
| Password type | Device default |
| Minimum password length |  |
| Maximum minutes of inactivity before password is required | Not configured |
| Password expiration (days) |  |
| Number of previous passwords to prevent reuse |  |
| Require password when device returns from idle state (Mobile and Holographic) | Not configured |
| Encryption | |
| Require encryption of data storage on device. | Not configured |
| Device Security | |
| Firewall | Not configured |
| Trusted Platform Module (TPM) | Not configured |
| Antivirus | Not configured |
| Antispyware | Not configured |
| Defender | |
| Microsoft Defender Antimalware | Not configured |
| Microsoft Defender Antimalware minimum version |  |
| Microsoft Defender Antimalware security intelligence up-to-date | Not configured |
| Real-time protection | Not configured |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint rules | |
| Require the device to be at or under the machine risk score: | Not configured |

Table 38. Settings - Win - Compliance - Default - C - Broad v1.0.0

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Schedule | Message template | Additional recipients (via email) |
| Mark device noncompliant | Immediately |  |  |

Table 39. Actions for noncompliance - Win - Compliance - Default - C - Broad v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 40. Assignments - Win - Compliance - Default - C - Broad v1.0.0

* + 1. Win - Compliance - U - Defender for Endpoint - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Compliance - U - Defender for Endpoint - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Windows 10 and later compliance policy |
| Created | 10 April 2025 09:23:11 |
| Last modified | 10 April 2025 09:23:11 |
| Version | 1 |
| Scope tags | Default |

Table 41. Basics - Win - Compliance - U - Defender for Endpoint - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Custom Compliance | |
| Custom compliance | Not configured |
| Device Health | |
| Windows 10 and 11 | |
| BitLocker | Not configured |
| Secure Boot | Not configured |
| Code integrity | Not configured |
| Windows 11 only | |
| Early Launch AntiMalware | Not configured |
| Firmware Protection | Not configured |
| Memory Integrity Protection | Not configured |
| Memory Access Protection | Not configured |
| Virtualization-based Security | Not configured |
| Device Properties | |
| Operating System Version | |
| Minimum OS version |  |
| Maximum OS version |  |
| Minimum OS version for mobile devices |  |
| Maximum OS version for mobile devices |  |
| Valid operating system builds |  |
| Configuration Manager Compliance | |
| Require device compliance from Configuration Manager | Not configured |
| System Security | |
| Password | |
| Require a password to unlock mobile devices | Not configured |
| Simple passwords | Not configured |
| Password type | Device default |
| Minimum password length |  |
| Maximum minutes of inactivity before password is required | Not configured |
| Password expiration (days) |  |
| Number of previous passwords to prevent reuse |  |
| Require password when device returns from idle state (Mobile and Holographic) | Not configured |
| Encryption | |
| Require encryption of data storage on device. | Not configured |
| Device Security | |
| Firewall | Not configured |
| Trusted Platform Module (TPM) | Not configured |
| Antivirus | Not configured |
| Antispyware | Not configured |
| Defender | |
| Microsoft Defender Antimalware | Require |
| Microsoft Defender Antimalware minimum version |  |
| Microsoft Defender Antimalware security intelligence up-to-date | Require |
| Real-time protection | Require |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint rules | |
| Require the device to be at or under the machine risk score: | Not configured |

Table 42. Settings - Win - Compliance - U - Defender for Endpoint - v1.0.0

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Schedule | Message template | Additional recipients (via email) |
| Mark device noncompliant | 0.25 days after noncompliance |  |  |

Table 43. Actions for noncompliance - Win - Compliance - U - Defender for Endpoint - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 44. Assignments - Win - Compliance - U - Defender for Endpoint - v1.0.0

* + 1. Win - Compliance - U - Device Health - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Compliance - U - Device Health - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Windows 10 and later compliance policy |
| Created | 10 April 2025 09:23:12 |
| Last modified | 10 April 2025 09:23:12 |
| Version | 1 |
| Scope tags | Default |

Table 45. Basics - Win - Compliance - U - Device Health - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Custom Compliance | |
| Custom compliance | Not configured |
| Device Health | |
| Windows 10 and 11 | |
| BitLocker | Require |
| Secure Boot | Require |
| Code integrity | Require |
| Windows 11 only | |
| Early Launch AntiMalware | Not configured |
| Firmware Protection | Not configured |
| Memory Integrity Protection | Not configured |
| Memory Access Protection | Not configured |
| Virtualization-based Security | Not configured |
| Device Properties | |
| Operating System Version | |
| Minimum OS version |  |
| Maximum OS version |  |
| Minimum OS version for mobile devices |  |
| Maximum OS version for mobile devices |  |
| Valid operating system builds |  |
| Configuration Manager Compliance | |
| Require device compliance from Configuration Manager | Not configured |
| System Security | |
| Password | |
| Require a password to unlock mobile devices | Not configured |
| Simple passwords | Not configured |
| Password type | Device default |
| Minimum password length |  |
| Maximum minutes of inactivity before password is required | Not configured |
| Password expiration (days) |  |
| Number of previous passwords to prevent reuse |  |
| Require password when device returns from idle state (Mobile and Holographic) | Not configured |
| Encryption | |
| Require encryption of data storage on device. | Not configured |
| Device Security | |
| Firewall | Not configured |
| Trusted Platform Module (TPM) | Not configured |
| Antivirus | Not configured |
| Antispyware | Not configured |
| Defender | |
| Microsoft Defender Antimalware | Not configured |
| Microsoft Defender Antimalware minimum version |  |
| Microsoft Defender Antimalware security intelligence up-to-date | Not configured |
| Real-time protection | Not configured |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint rules | |
| Require the device to be at or under the machine risk score: | Not configured |

Table 46. Settings - Win - Compliance - U - Device Health - v1.0.0

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Schedule | Message template | Additional recipients (via email) |
| Mark device noncompliant | 0.5 days after noncompliance |  |  |

Table 47. Actions for noncompliance - Win - Compliance - U - Device Health - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 48. Assignments - Win - Compliance - U - Device Health - v1.0.0

* + 1. Win - Compliance - U - Device Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Compliance - U - Device Security - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Windows 10 and later compliance policy |
| Created | 10 April 2025 09:23:13 |
| Last modified | 10 April 2025 09:23:13 |
| Version | 1 |
| Scope tags | Default |

Table 49. Basics - Win - Compliance - U - Device Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Custom Compliance | |
| Custom compliance | Not configured |
| Device Health | |
| Windows 10 and 11 | |
| BitLocker | Not configured |
| Secure Boot | Not configured |
| Code integrity | Not configured |
| Windows 11 only | |
| Early Launch AntiMalware | Not configured |
| Firmware Protection | Not configured |
| Memory Integrity Protection | Not configured |
| Memory Access Protection | Not configured |
| Virtualization-based Security | Not configured |
| Device Properties | |
| Operating System Version | |
| Minimum OS version |  |
| Maximum OS version |  |
| Minimum OS version for mobile devices |  |
| Maximum OS version for mobile devices |  |
| Valid operating system builds |  |
| Configuration Manager Compliance | |
| Require device compliance from Configuration Manager | Not configured |
| System Security | |
| Password | |
| Require a password to unlock mobile devices | Not configured |
| Simple passwords | Not configured |
| Password type | Device default |
| Minimum password length |  |
| Maximum minutes of inactivity before password is required | Not configured |
| Password expiration (days) |  |
| Number of previous passwords to prevent reuse |  |
| Require password when device returns from idle state (Mobile and Holographic) | Not configured |
| Encryption | |
| Require encryption of data storage on device. | Not configured |
| Device Security | |
| Firewall | Require |
| Trusted Platform Module (TPM) | Require |
| Antivirus | Require |
| Antispyware | Require |
| Defender | |
| Microsoft Defender Antimalware | Not configured |
| Microsoft Defender Antimalware minimum version |  |
| Microsoft Defender Antimalware security intelligence up-to-date | Not configured |
| Real-time protection | Not configured |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint rules | |
| Require the device to be at or under the machine risk score: | Not configured |

Table 50. Settings - Win - Compliance - U - Device Security - v1.0.0

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Schedule | Message template | Additional recipients (via email) |
| Mark device noncompliant | 0.25 days after noncompliance |  |  |

Table 51. Actions for noncompliance - Win - Compliance - U - Device Security - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 52. Assignments - Win - Compliance - U - Device Security - v1.0.0

* + 1. Win - Compliance - U - Password - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Compliance - U - Password - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Windows 10 and later compliance policy |
| Created | 10 April 2025 09:23:14 |
| Last modified | 10 April 2025 09:23:14 |
| Version | 1 |
| Scope tags | Default |

Table 53. Basics - Win - Compliance - U - Password - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Custom Compliance | |
| Custom compliance | Not configured |
| Device Health | |
| Windows 10 and 11 | |
| BitLocker | Not configured |
| Secure Boot | Not configured |
| Code integrity | Not configured |
| Windows 11 only | |
| Early Launch AntiMalware | Not configured |
| Firmware Protection | Not configured |
| Memory Integrity Protection | Not configured |
| Memory Access Protection | Not configured |
| Virtualization-based Security | Not configured |
| Device Properties | |
| Operating System Version | |
| Minimum OS version |  |
| Maximum OS version |  |
| Minimum OS version for mobile devices |  |
| Maximum OS version for mobile devices |  |
| Valid operating system builds |  |
| Configuration Manager Compliance | |
| Require device compliance from Configuration Manager | Not configured |
| System Security | |
| Password | |
| Require a password to unlock mobile devices | Require |
| Simple passwords | Block |
| Password type | Numeric |
| Minimum password length | 8 |
| Maximum minutes of inactivity before password is required | 15 minutes |
| Password expiration (days) |  |
| Number of previous passwords to prevent reuse |  |
| Require password when device returns from idle state (Mobile and Holographic) | Not configured |
| Encryption | |
| Require encryption of data storage on device. | Not configured |
| Device Security | |
| Firewall | Not configured |
| Trusted Platform Module (TPM) | Not configured |
| Antivirus | Not configured |
| Antispyware | Not configured |
| Defender | |
| Microsoft Defender Antimalware | Not configured |
| Microsoft Defender Antimalware minimum version |  |
| Microsoft Defender Antimalware security intelligence up-to-date | Not configured |
| Real-time protection | Not configured |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint rules | |
| Require the device to be at or under the machine risk score: | Not configured |

Table 54. Settings - Win - Compliance - U - Password - v1.0.0

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Schedule | Message template | Additional recipients (via email) |
| Mark device noncompliant | Immediately |  |  |

Table 55. Actions for noncompliance - Win - Compliance - U - Password - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 56. Assignments - Win - Compliance - U - Password - v1.0.0

1. Windows enrollment
   1. Autopilot
      1. StAH Shared Device Entra ID Joined Self Deploying

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH Shared Device Entra ID Joined Self Deploying |
| Description |  |
| Profile type | Windows Autopilot deployment profiles |
| Convert all targeted devices to Autopilot | No |
| Device type | Windows PC |
| Created | 15 April 2025 14:28:51 |
| Last modified | 15 April 2025 14:28:51 |
| Scope tags | Default |

Table 57. Basics - StAH Shared Device Entra ID Joined Self Deploying

|  |  |
| --- | --- |
| Name | Value |
| Out-of-box experience (OOBE) | |
| Deployment mode | Self-Deploying |
| Join to Microsoft Entra ID as | Microsoft Entra joined |
| Language (Region) | English (United Kingdom) |
| Automatically configure keyboard | Yes |
| Microsoft Software License Terms | Hide |
| Privacy settings | Hide |
| Hide change account options | Hide |
| User account type | Standard |
| Allow pre-provisioned deployment | No |
| Apply device name template | Yes |
| Enter a name | W11-%SERIAL% |

Table 58. Settings - StAH Shared Device Entra ID Joined Self Deploying

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Dynamic Group-Shared Entra ID Device | None | None |

Table 59. Assignments - StAH Shared Device Entra ID Joined Self Deploying

* + 1. StAH Standard Device Entra ID Joined

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH Standard Device Entra ID Joined |
| Description |  |
| Profile type | Windows Autopilot deployment profiles |
| Convert all targeted devices to Autopilot | No |
| Device type | Windows PC |
| Created | 08 April 2025 13:56:03 |
| Last modified | 08 April 2025 13:56:03 |
| Scope tags | Default |

Table 60. Basics - StAH Standard Device Entra ID Joined

|  |  |
| --- | --- |
| Name | Value |
| Out-of-box experience (OOBE) | |
| Deployment mode | User-Driven |
| Join to Microsoft Entra ID as | Microsoft Entra joined |
| Language (Region) | English (United Kingdom) |
| Automatically configure keyboard | Yes |
| Microsoft Software License Terms | Hide |
| Privacy settings | Hide |
| Hide change account options | Hide |
| User account type | Standard |
| Allow pre-provisioned deployment | No |
| Apply device name template | Yes |
| Enter a name | W11-%SERIAL% |

Table 61. Settings - StAH Standard Device Entra ID Joined

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Dynamic Group-Standard Entra ID Device | None | None |
| STAH-Intune-ModernDesktopAutopilotDeploy | None | None |

Table 62. Assignments - StAH Standard Device Entra ID Joined

* 1. Enrollment Status Page
     1. All users and all devices

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | All users and all devices |
| Description | This is the default enrollment status screen configuration applied with the lowest priority to all users and all devices regardless of group membership. |
| Policy type | Enrollment Status Page |
| Created | 01 January 0001 00:00:00 |
| Last modified | 25 March 2025 11:20:55 |

Table 63. Basics - All users and all devices

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Show app and profile configuration progress | No |
| Show an error when installation takes longer than specified number of minutes | 0 |
| Show custom message when time limit or error occurs | No |
| Turn on log collection and diagnostics page for end users | No |
| Only show page to devices provisioned by out-of-box experience (OOBE) | No |
| Block device use until all apps and profiles are installed | No |

Table 64. Settings - All users and all devices

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 65. Assignments - All users and all devices

* + 1. StAH Standard Device Entra ID Joined

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH Standard Device Entra ID Joined |
| Description |  |
| Policy type | Enrollment Status Page |
| Created | 08 April 2025 13:57:19 |
| Last modified | 15 July 2025 10:17:45 |
| Version | 21 |
| Scope tags | Default |

Table 66. Basics - StAH Standard Device Entra ID Joined

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Show app and profile configuration progress | Yes |
| Show an error when installation takes longer than specified number of minutes | 90 |
| Show custom message when time limit or error occurs | Yes |
| Error message | Setup could not be completed. Please try again or contact your support person for help. |
| Turn on log collection and diagnostics page for end users | No |
| Only show page to devices provisioned by out-of-box experience (OOBE) | Yes |
| Block device use until all apps and profiles are installed | Yes |
| Allow users to reset device if installation error occurs | Yes |
| Allow users to use device if installation error occurs | Yes |
| Block device use until required apps are installed if they are assigned to the user/device | Cisco Secure Client - AnyConnect VPN - No Autoconnect  Egress Outlook Add-in 24.8.1833  Imprivata Agent v25.1.001.26  Microsoft 365 Apps for Business - Win32  SenseOn SEE Agent v6.11.45  Specops Authentication Client v7.20.24179.1  [TS] Forcepoint One Endpoint v24.07.5688 |

Table 67. Settings - StAH Standard Device Entra ID Joined

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 68. Assignments - StAH Standard Device Entra ID Joined

* + 1. StAH Standard Device Entra ID Joined - UAT

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | StAH Standard Device Entra ID Joined - UAT |
| Description |  |
| Policy type | Enrollment Status Page |
| Created | 04 July 2025 14:45:27 |
| Last modified | 15 July 2025 10:17:27 |
| Version | 6 |
| Scope tags | Default |

Table 69. Basics - StAH Standard Device Entra ID Joined - UAT

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Show app and profile configuration progress | Yes |
| Show an error when installation takes longer than specified number of minutes | 90 |
| Show custom message when time limit or error occurs | Yes |
| Error message | Setup could not be completed. Please try again or contact your support person for help. |
| Turn on log collection and diagnostics page for end users | No |
| Only show page to devices provisioned by out-of-box experience (OOBE) | Yes |
| Block device use until all apps and profiles are installed | Yes |
| Allow users to reset device if installation error occurs | Yes |
| Allow users to use device if installation error occurs | Yes |
| Block device use until required apps are installed if they are assigned to the user/device | Cisco Secure Client v5.1.7.80 - Entra  Egress Outlook Add-in 24.8.1833  Imprivata Agent v25.1.001.26  Microsoft 365 Apps for Business - Win32  SenseOn SEE Agent v6.11.45  Specops Authentication Client v7.20.24179.1  [TS] Forcepoint One Endpoint v24.07.5688 |

Table 70. Settings - StAH Standard Device Entra ID Joined - UAT

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Test-Autopilot-UAT | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 71. Assignments - StAH Standard Device Entra ID Joined - UAT

1. Driver updates for Windows 10 and later
   1. Driver Update Profiles
      1. Win - Updates - U - Driver Update - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Driver Update - Broad Ring - v1.0 |
| Description |  |
| Policy type | Automatic approval driver update policy |
| Created | 17 June 2025 10:11:41 |
| Last modified | 17 June 2025 10:11:41 |
| Scope tags | Default |

Table 72. Basics - Win - Updates - U - Driver Update - Broad Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Approval method: | Automatically approve all recommended driver updates |
| Make updates available after | 14 days |

Table 73. Settings - Win - Updates - U - Driver Update - Broad Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Default-Broad-Devices | None | None |
| Excluded Groups | | |
| Intune-Update-Preview-UAT |  |  |
| Intune-Updates-Preview-Devices |  |  |

Table 74. Assignments - Win - Updates - U - Driver Update - Broad Ring - v1.0

* + 1. Win - Updates - U - Driver Update - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Driver Update - Pilot Ring - v1.0 |
| Description |  |
| Policy type | Automatic approval driver update policy |
| Created | 21 March 2025 09:01:47 |
| Last modified | 21 March 2025 09:01:47 |
| Scope tags | Default |

Table 75. Basics - Win - Updates - U - Driver Update - Pilot Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Approval method: | Automatically approve all recommended driver updates |
| Make updates available after | 7 days |

Table 76. Settings - Win - Updates - U - Driver Update - Pilot Ring - v1.0

* + 1. Win - Updates - U - Driver Update - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Driver Update - Preview Ring - v1.0 |
| Description |  |
| Policy type | Automatic approval driver update policy |
| Created | 21 March 2025 09:01:47 |
| Last modified | 21 March 2025 09:01:47 |
| Scope tags | Default |

Table 77. Basics - Win - Updates - U - Driver Update - Preview Ring - v1.0

|  |  |
| --- | --- |
| Name | Value |
| Settings | |
| Approval method: | Automatically approve all recommended driver updates |
| Make updates available after | 1 days |

Table 78. Settings - Win - Updates - U - Driver Update - Preview Ring - v1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Update-Preview-UAT | None | None |
| Intune-Updates-Preview-Devices | None | None |

Table 79. Assignments - Win - Updates - U - Driver Update - Preview Ring - v1.0

1. Device configuration
   1. Settings Catalog
      1. Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules |
| Description | Test policy as other policy is not deployiing |
| Profile type | Settings catalog |
| Category | Firewall |
| Policy type | Windows Firewall Rules |
| Platform supported | Windows 10 and later |
| Created | 14 May 2025 14:48:25 |
| Last modified | 20 May 2025 16:26:04 |
| Scope tags | Default |

Table 80. Basics - Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules

|  |  |
| --- | --- |
| Name | Value |
| Firewall | |
| Enabled | Enabled |
| Name | File and Printer Sharing (SMB-In) |
| Local Port Ranges | 445 |
| Local Address Ranges | \* |
| Direction | The rule applies to inbound traffic. |
| Remote Address Ranges | LocalSubnet |
| Action | Allow |
| Protocol | 6 |

Table 81. Settings - Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| StAH-Windows11-PoC-D-Firewall Testing | None | None |

Table 82. Assignments - Win - Windows Firewall - D - Firewall Rules - Test Windows Firewall Rules

* + 1. \*\*Win - Device Security - U - Windows Spotlight and Org Messages - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Device Security - U - Windows Spotlight and Org Messages - v1.0.0 |
| Description | As per Ellis on 7th April 2025, Spotlight to be blocked. CIS will handle this. |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:24 |
| Last modified | 02 May 2025 16:29:54 |
| Scope tags | Default |

Table 83. Basics - \*\*Win - Device Security - U - Windows Spotlight and Org Messages - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Experience | |
| Allow Spotlight Collection (User) | 0 |
| Allow Windows Spotlight (User) | Allow |
| Allow Tailored Experiences With Diagnostic Data (User) | Allow |
| Allow Third Party Suggestions In Windows Spotlight (User) | Block |
| Allow Windows Consumer Features | Block |
| Allow Windows Spotlight On Action Center (User) | Allow |
| Allow Windows Spotlight Windows Welcome Experience (User) | Block |
| Allow Windows Tips | Allow |
| Configure Windows Spotlight On Lock Screen (User) | Windows spotlight disabled. |
| Allow Windows Spotlight On Settings (User) | Block |
| Disable Cloud Optimized Content | Disabled |
| Enable delivery of organizational messages (User) | Enabled |

Table 84. Settings - \*\*Win - Device Security - U - Windows Spotlight and Org Messages - v1.0.0

* + 1. \*\*Win - Encryption - U - Personal Data Encryption - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Encryption - U - Personal Data Encryption - v1.0.0 |
| Description | Removed, as PDE requires Windows Hello which we have disabled.  NOTE: PDE is only applicable to Windows 11 22H2 or higher, Entra-Joined devices and does not work on Windows Pro/Business SKU's:  https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/personal-data-encryption/ |
| Profile type | Settings catalog |
| Category | Disk encryption |
| Policy type | Personal Data Encryption |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:25 |
| Last modified | 20 June 2025 16:21:18 |
| Scope tags | Default |

Table 85. Basics - \*\*Win - Encryption - U - Personal Data Encryption - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Personal Data Encryption | |
| Enable Personal Data Encryption (User) | Enable Personal Data Encryption. |
| Protect Pictures (User) (Windows Insiders only) | Enable Personal Data Encryption on the folder. |
| Protect Documents (User) (Windows Insiders only) | Enable Personal Data Encryption on the folder. |
| Protect Desktop (User) (Windows Insiders only) | Enable Personal Data Encryption on the folder. |

Table 86. Settings - \*\*Win - Encryption - U - Personal Data Encryption - v1.0.0

* + 1. \*\*Win - Microsoft Edge - D - Enterprise Mode Cloud Site List - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Microsoft Edge - D - Enterprise Mode Cloud Site List - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:30 |
| Last modified | 10 April 2025 21:38:17 |
| Scope tags | Default |

Table 87. Basics - \*\*Win - Microsoft Edge - D - Enterprise Mode Cloud Site List - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Configure Internet Explorer integration | Enabled |
| Configure Internet Explorer integration (Device) | Internet Explorer mode |
| Configure the Enterprise Mode Cloud Site List | Enabled |
| Configure the Enterprise Mode Cloud Site List (Device) | 9b846c32-c074-4de6-b4d6-bd0a1c6741c2 |

Table 88. Settings - \*\*Win - Microsoft Edge - D - Enterprise Mode Cloud Site List - v1.0.0

* + 1. \*\*Win - Windows Hello for Business - D - Cloud Kerberos Trust - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Windows Hello for Business - D - Cloud Kerberos Trust - v1.0.0 |
| Description | NOTE: Requires setup of Cloud Kerberos Trust to function.  https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/deploy/hybrid-cloud-kerberos-trust |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:46 |
| Last modified | 10 April 2025 21:54:58 |
| Scope tags | Default |

Table 89. Basics - \*\*Win - Windows Hello for Business - D - Cloud Kerberos Trust - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Kerberos | |
| Cloud Kerberos Ticket Retrieval Enabled | Enabled |
| Windows Hello For Business | |
| Use Cloud Trust For On Prem Auth | Enabled |

Table 90. Settings - \*\*Win - Windows Hello for Business - D - Cloud Kerberos Trust - v1.0.0

* + 1. \*\*Win - Windows Hello for Business - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Windows Hello for Business - D - Configuration - v1.0.0 |
| Description | Removed assignment on 040625 as per Peter H |
| Profile type | Settings catalog |
| Category | Account protection |
| Policy type | Account Protection |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:47 |
| Last modified | 04 June 2025 13:40:12 |
| Scope tags | Default |

Table 91. Basics - \*\*Win - Windows Hello for Business - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Windows Hello For Business | |
| Require Security Device | true |
| Use Windows Hello For Business (Device) | true |
| Minimum PIN Length | 6 |
| Use Certificate For On Prem Auth | Disabled |
| Enable Pin Recovery | true |
| Facial Features Use Enhanced Anti Spoofing | true |

Table 92. Settings - \*\*Win - Windows Hello for Business - D - Configuration - v1.0.0

* + 1. \*\*X - Win - Dispensation - CIS -L1 - Bitlocker - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*X - Win - Dispensation - CIS -L1 - Bitlocker - D - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:48 |
| Last modified | 10 April 2025 21:55:20 |
| Scope tags | Default |

Table 93. Basics - \*\*X - Win - Dispensation - CIS -L1 - Bitlocker - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Device Installation Restrictions | |
| Allow administrators to override Device Installation Restriction policies | Enabled |
| Prevent installation of devices that match any of these device IDs | Disabled |
| Prevent installation of devices using drivers that match these device setup classes | Disabled |
| Display a custom message title when device installation is prevented by a policy setting | Enabled |
| Main Text (Device) | CIS Policy |
| Display a custom message when installation is prevented by a policy setting | Enabled |
| Detail Text (Device) | CIS Device Installation Policy |

Table 94. Settings - \*\*X - Win - Dispensation - CIS -L1 - Bitlocker - D - v1.0.0

* + 1. \*\*X - Win - Dispensation - CIS -L2 - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*X - Win - Dispensation - CIS -L2 - D - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:48 |
| Last modified | 10 April 2025 21:55:33 |
| Scope tags | Default |

Table 95. Basics - \*\*X - Win - Dispensation - CIS -L2 - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Sleep Settings | |
| Allow standby states (S1-S3) when sleeping (on battery) | Enabled |
| Allow standby states (S1-S3) when sleeping (plugged in) | Enabled |
| Camera | |
| Allow Camera | Allowed. |
| Administrative Templates | |
| Store | |
| Turn off the Store application | Disabled |
| Credential User Interface | |
| Require trusted path for credential entry | Disabled |

Table 96. Settings - \*\*X - Win - Dispensation - CIS -L2 - D - v1.0.0

* + 1. \*Win - Windows LAPS - D - LAPS Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*Win - Windows LAPS - D - LAPS Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Account protection |
| Policy type | Local admin password solution (Windows LAPS) |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:47 |
| Last modified | 17 June 2025 13:21:44 |
| Scope tags | Default |

Table 97. Basics - \*Win - Windows LAPS - D - LAPS Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Backup Directory | Backup the password to Azure AD only |
| Password Age Days | 7 |
| Password Complexity | Large letters + small letters + numbers + special characters (improved readability) |
| Password Length | 21 |
| Post Authentication Actions | Reset the password and logoff the managed account: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminated. |
| Post Authentication Reset Delay | 1 |

Table 98. Settings - \*Win - Windows LAPS - D - LAPS Configuration - v1.0.0

* + 1. Win - CIS - Level 2 - Admin Templates - D - v3.0.1

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - CIS - Level 2 - Admin Templates - D - v3.0.1 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:09 |
| Last modified | 10 April 2025 09:27:09 |
| Scope tags | Default |

Table 99. Basics - Win - CIS - Level 2 - Admin Templates - D - v3.0.1

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| MSS (Legacy) | |
| MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended) | Enabled |
| MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | Enabled |
| KeepAliveTime (Device) | 300000 or 5 minutes (recommended) |
| MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Disabled |
| MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | Enabled |
| TcpMaxDataRetransmissions (Device) | 3 |
| MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | Enabled |
| TcpMaxDataRetransmissions (Device) | 3 |
| Link-Layer Topology Discovery | |
| Turn on Mapper I/O (LLTDIO) driver | Disabled |
| Turn on Responder (RSPNDR) driver | Disabled |
| Windows Connect Now | |
| Configuration of wireless settings using Windows Connect Now | Disabled |
| Prohibit access of the Windows Connect Now wizards | Enabled |
| Internet Communication settings | |
| Turn off access to the Store | Enabled |
| Turn off Help Experience Improvement Program (User) | Enabled |
| Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com | Enabled |
| Turn off printing over HTTP | Enabled |
| Turn off Registration if URL connection is referring to Microsoft.com | Enabled |
| Turn off Search Companion content file updates | Enabled |
| Turn off the "Order Prints" picture task | Enabled |
| Turn off the "Publish to Web" task for files and folders | Enabled |
| Turn off the Windows Messenger Customer Experience Improvement Program | Enabled |
| Turn off Windows Customer Experience Improvement Program | Enabled |
| Turn off Windows Error Reporting | Enabled |
| Kerberos | |
| Support device authentication using certificate | Enabled |
| Device authentication behavior using certificate: (Device) | Automatic |
| Locale Services | |
| Disallow copying of user input methods to the system account for sign-in | Enabled |
| Microsoft Support Diagnostic Tool | |
| Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider | Disabled |
| App runtime | |
| Block launching Universal Windows apps with Windows Runtime API access from hosted content. | Enabled |
| MAPS | |
| Join Microsoft MAPS | Disabled |
| Reporting | |
| Configure Watson events | Disabled |
| Push To Install | |
| Turn off Push To Install service | Enabled |
| Connections | |
| Allow users to connect remotely by using Remote Desktop Services | Disabled |
| Device and Resource Redirection | |
| Do not allow COM port redirection | Enabled |
| Do not allow LPT port redirection | Enabled |
| Do not allow supported Plug and Play device redirection | Enabled |
| Session Time Limits | |
| Set time limit for active but idle Remote Desktop Services sessions | Enabled |
| Idle session limit: (Device) | 15 minutes |
| Set time limit for disconnected sessions | Enabled |
| End a disconnected session (Device) | 1 minute |
| Store | |
| Turn off the Store application | Disabled |
| Windows Installer | |
| Prevent Internet Explorer security prompt for Windows Installer scripts | Disabled |
| Playback | |
| Prevent Codec Download (User) | Enabled |
| WinRM Service | |
| Allow remote server management through WinRM | Disabled |
| Windows Remote Shell | |
| Allow Remote Shell Access | Disabled |

Table 100. Settings - Win - CIS - Level 2 - Admin Templates - D - v3.0.1

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 101. Assignments - Win - CIS - Level 2 - Admin Templates - D - v3.0.1

* + 1. Win - CIS - Level 2 - No Services - D - v3.0.1

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - CIS - Level 2 - No Services - D - v3.0.1 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:09 |
| Last modified | 11 April 2025 13:03:01 |
| Scope tags | Default |

Table 102. Basics - Win - CIS - Level 2 - No Services - D - v3.0.1

|  |  |
| --- | --- |
| Name | Value |
| Camera | |
| Allow Camera | Allowed. |
| Defender | |
| Enable File Hash Computation | Enable |
| Experience | |
| Allow Windows Spotlight (User) | Block |
| Licensing | |
| Disallow KMS Client Online AVS Validation | Allow |
| Local Policies Security Options | |
| Devices Prevent Users From Installing Printer Drivers When Connecting To Shared Printers | Enable |
| Microsoft App Store | |
| Disable Store Originated Apps | Disabled |
| Privacy | |
| Allow Cross Device Clipboard | Block |
| Disable Advertising ID | Enabled |
| Upload User Activities | Disabled |
| Search | |
| Allow Cloud Search | Allowed. |
| Allow Search Highlights | 0 |
| Settings | |
| Allow Online Tips | Block |
| System | |
| Allow Font Providers | Not allowed. No traffic to fs.microsoft.com and only locally installed fonts are available. |
| Disable One Drive File Sync | Sync enabled. |
| Windows Ink Workspace | |
| Allow Suggested Apps In Windows Ink Workspace | Block |

Table 103. Settings - Win - CIS - Level 2 - No Services - D - v3.0.1

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 104. Assignments - Win - CIS - Level 2 - No Services - D - v3.0.1

* + 1. Win - Defender Antivirus - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Defender Antivirus - D - Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Antivirus |
| Policy type | Microsoft Defender Antivirus |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:11 |
| Last modified | 17 June 2025 13:33:14 |
| Scope tags | Default |

Table 105. Basics - Win - Defender Antivirus - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Allow Archive Scanning | Allowed. Scans the archive files. |
| Allow Behavior Monitoring | Allowed. Turns on real-time behavior monitoring. |
| Allow Cloud Protection | Allowed. Turns on Cloud Protection. |
| Allow Email Scanning | Allowed. Turns on email scanning. |
| Allow Full Scan Removable Drive Scanning | Allowed. Scans removable drives. |
| Allow scanning of all downloaded files and attachments | Allowed. |
| Allow Realtime Monitoring | Allowed. Turns on and runs the real-time monitoring service. |
| Allow Scanning Network Files | Allowed. Scans network files. |
| Allow Script Scanning | Allowed. |
| Allow User UI Access | Allowed. Lets users access UI. |
| Check For Signatures Before Running Scan | Enabled |
| Cloud Block Level | High |
| Cloud Extended Timeout | 50 |
| Disable Catchup Full Scan | Disabled |
| Disable Catchup Quick Scan | Disabled |
| Enable Low CPU Priority | Enabled |
| Enable Network Protection | Enabled (block mode) |
| PUA Protection | PUA Protection on. Detected items are blocked. They will show in history along with other threats. |
| Real Time Scan Direction | Monitor all files (bi-directional). |
| Schedule Quick Scan Time | 660 |
| Signature Update Interval | 1 |
| Submit Samples Consent | Send safe samples automatically. |
| Disable Local Admin Merge | Disable Local Admin Merge |
| Allow On Access Protection | Allowed. |
| Remediation action for High severity threats | Remove. Removes files from system. |
| Remediation action for Severe threats | Remove. Removes files from system. |
| Remediation action for Low severity threats | Block. Blocks file execution. |
| Remediation action for Moderate severity threats | Remove. Removes files from system. |
| Metered Connection Updates | Allowed |

Table 106. Settings - Win - Defender Antivirus - D - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 107. Assignments - Win - Defender Antivirus - D - Configuration - v1.0.0

* + 1. Win - Defender Antivirus - D - Security Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Defender Antivirus - D - Security Experience - v1.0.0 |
| Description | NOTE: The "Tamper Protection" setting requires an active Defender for Endpoint P1/P2 or Defender for Business license.  https://learn.microsoft.com/en-us/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection |
| Profile type | Settings catalog |
| Category | Antivirus |
| Policy type | Windows Security Experience |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:11 |
| Last modified | 17 June 2025 13:32:56 |
| Scope tags | Default |

Table 108. Basics - Win - Defender Antivirus - D - Security Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| TamperProtection (Device) | On |
| Windows Defender Security Center | |
| Disable Family UI | (Enable) The users cannot see the display of the family options area in Windows Defender Security Center. |
| Disable Enhanced Notifications | (Disable) Windows Defender Security Center will display critical and non-critical notifications to users.. |
| Hide Windows Security Notification Area Control | Disabled |

Table 109. Settings - Win - Defender Antivirus - D - Security Experience - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 110. Assignments - Win - Defender Antivirus - D - Security Experience - v1.0.0

* + 1. Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0 |
| Description | Added Temp for reporting purposes from existing devices - Ellis Barrett |
| Profile type | Settings catalog |
| Category | Attack surface reduction |
| Policy type | Attack Surface Reduction Rules |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:12 |
| Last modified | 02 July 2025 15:06:09 |
| Scope tags | Default |

Table 111. Basics - Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Block execution of potentially obfuscated scripts | Audit |
| Block Win32 API calls from Office macros | Audit |
| Block executable files from running unless they meet a prevalence, age, or trusted list criterion | Audit |
| Block Office communication application from creating child processes | Audit |
| Block all Office applications from creating child processes | Audit |
| Block Adobe Reader from creating child processes | Audit |
| Block credential stealing from the Windows local security authority subsystem | Audit |
| Block JavaScript or VBScript from launching downloaded executable content | Audit |
| Block untrusted and unsigned processes that run from USB | Audit |
| Block persistence through WMI event subscription | Audit |
| Block use of copied or impersonated system tools | Audit |
| Block abuse of exploited vulnerable signed drivers (Device) | Audit |
| Block process creations originating from PSExec and WMI commands | Audit |
| Block Office applications from creating executable content | Audit |
| Block Office applications from injecting code into other processes | Audit |
| Block rebooting machine in Safe Mode | Audit |
| Use advanced protection against ransomware | Audit |
| Block executable content from email client and webmail | Audit |
| Enable Controlled Folder Access | Audit Mode |

Table 112. Settings - Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 113. Assignments - Win - Defender Attack Surface Reduction - D - ASR Rules (Audit Mode) - v1.0.0

* + 1. Win - Defender Attack Surface Reduction - D - ASR Rules (Block Mode) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Defender Attack Surface Reduction - D - ASR Rules (Block Mode) - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Attack surface reduction |
| Policy type | Attack Surface Reduction Rules |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:12 |
| Last modified | 02 July 2025 15:06:26 |
| Scope tags | Default |

Table 114. Basics - Win - Defender Attack Surface Reduction - D - ASR Rules (Block Mode) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Block execution of potentially obfuscated scripts | Block |
| Block Win32 API calls from Office macros | Audit |
| Block executable files from running unless they meet a prevalence, age, or trusted list criterion | Block |
| Block Office communication application from creating child processes | Block |
| Block all Office applications from creating child processes | Block |
| Block Adobe Reader from creating child processes | Block |
| Block credential stealing from the Windows local security authority subsystem | Block |
| Block JavaScript or VBScript from launching downloaded executable content | Block |
| Block Webshell creation for Servers | Block |
| Block untrusted and unsigned processes that run from USB | Block |
| Block persistence through WMI event subscription | Block |
| Block use of copied or impersonated system tools | Block |
| Block abuse of exploited vulnerable signed drivers (Device) | Block |
| Block process creations originating from PSExec and WMI commands | Block |
| Block Office applications from creating executable content | Block |
| Block Office applications from injecting code into other processes | Block |
| Block rebooting machine in Safe Mode | Block |
| Use advanced protection against ransomware | Block |
| Block executable content from email client and webmail | Block |
| Enable Controlled Folder Access | Enabled |

Table 115. Settings - Win - Defender Attack Surface Reduction - D - ASR Rules (Block Mode) - v1.0.0

* + 1. Win - Device Security - D - Audit and Event Logging - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Audit and Event Logging - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:14 |
| Last modified | 10 April 2025 09:27:14 |
| Scope tags | Default |

Table 116. Basics - Win - Device Security - D - Audit and Event Logging - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Application | |
| Control Event Log behavior when the log file reaches its maximum size | Disabled |
| Specify the maximum log file size (KB) | Enabled |
| Maximum Log Size (KB) | 32768 |
| Security | |
| Control Event Log behavior when the log file reaches its maximum size | Disabled |
| Specify the maximum log file size (KB) | Enabled |
| Maximum Log Size (KB) | 196608 |
| Setup | |
| Control Event Log behavior when the log file reaches its maximum size | Disabled |
| Specify the maximum log file size (KB) | Enabled |
| Maximum Log Size (KB) (Device) | 32768 |
| System | |
| Control Event Log behavior when the log file reaches its maximum size | Disabled |
| Specify the maximum log file size (KB) | Enabled |
| Maximum Log Size (KB) | 32768 |
| Auditing | |
| Account Logon Audit Credential Validation | Success+ Failure |
| Account Logon Logoff Audit Account Lockout | Failure |
| Account Logon Logoff Audit Group Membership | Success |
| Account Logon Logoff Audit Logoff | Success |
| Account Logon Logoff Audit Logon | Success+ Failure |
| Account Management Audit Application Group Management | Success+ Failure |
| Audit Authentication Policy Change | Success |
| Audit Authorization Policy Change | Success |
| Audit Changes to Audit Policy | Success |
| Audit File Share Access | Success+Failure |
| Audit Other Logon Logoff Events | Success+Failure |
| Audit Security Group Management | Success |
| Audit Security System Extension | Success |
| Audit Special Logon | Success |
| Audit User Account Management | Success+Failure |
| Detailed Tracking Audit PNP Activity | Success |
| Detailed Tracking Audit Process Creation | Success |
| Object Access Audit Detailed File Share | Failure |
| Object Access Audit Other Object Access Events | Success+ Failure |
| Object Access Audit Removable Storage | Success+ Failure |
| Policy Change Audit MPSSVC Rule Level Policy Change | Success+ Failure |
| Policy Change Audit Other Policy Change Events | Failure |
| Privilege Use Audit Sensitive Privilege Use | Success+ Failure |
| System Audit I Psec Driver | Success+ Failure |
| System Audit Other System Events | Success+ Failure |
| System Audit Security State Change | Success |
| System Audit System Integrity | Success+ Failure |

Table 117. Settings - Win - Device Security - D - Audit and Event Logging - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 118. Assignments - Win - Device Security - D - Audit and Event Logging - v1.0.0

* + 1. Win - Device Security - D - Config Refresh - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Config Refresh - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:14 |
| Last modified | 10 April 2025 09:27:14 |
| Scope tags | Default |

Table 119. Basics - Win - Device Security - D - Config Refresh - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Config Refresh | |
| Config refresh | Enabled. |
| Refresh cadence | 30 |

Table 120. Settings - Win - Device Security - D - Config Refresh - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 121. Assignments - Win - Device Security - D - Config Refresh - v1.0.0

* + 1. Win - Device Security - D - Enhanced Phishing Protection - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Enhanced Phishing Protection - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:14 |
| Last modified | 10 April 2025 09:27:14 |
| Scope tags | Default |

Table 122. Basics - Win - Device Security - D - Enhanced Phishing Protection - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Smart Screen | |
| Enhanced Phishing Protection | |
| Notify Malicious | Enabled |
| Notify Password Reuse | Enabled |
| Notify Unsafe App | Enabled |
| Service Enabled | Enabled |

Table 123. Settings - Win - Device Security - D - Enhanced Phishing Protection - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 124. Assignments - Win - Device Security - D - Enhanced Phishing Protection - v1.0.0

* + 1. Win - Device Security - D - Local Security Policies - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Local Security Policies - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:15 |
| Last modified | 10 April 2025 09:27:15 |
| Scope tags | Default |

Table 125. Basics - Win - Device Security - D - Local Security Policies - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Local Policies Security Options | |
| Accounts Enable Administrator Account Status | Enable |
| Accounts Enable Guest Account Status | Disable |
| Accounts Limit Local Account Use Of Blank Passwords To Console Logon Only | Enabled |
| Interactive Logon Smart Card Removal Behavior | Lock Workstation |
| Microsoft Network Client Digitally Sign Communications Always | Enable |
| Microsoft Network Client Send Unencrypted Password To Third Party SMB Servers | Disable |
| Microsoft Network Server Digitally Sign Communications Always | Enable |
| Network Access Do Not Allow Anonymous Enumeration Of SAM Accounts | Enabled |
| Network Access Do Not Allow Anonymous Enumeration Of Sam Accounts And Shares | Enabled |
| Network Access Restrict Anonymous Access To Named Pipes And Shares | Enable |
| Network Access Restrict Clients Allowed To Make Remote Calls To SAM | O:BAG:BAD:(A;;RC;;;BA) |
| Network Security Do Not Store LAN Manager Hash Value On Next Password Change | Enable |
| Network Security LAN Manager Authentication Level | Send NTLMv2 responses only. Refuse LM and NTLM |
| Network Security Minimum Session Security For NTLMSSP Based Clients | Require NTLM and 128-bit encryption |
| Network Security Minimum Session Security For NTLMSSP Based Servers | Require NTLM and 128-bit encryption |
| User Account Control Behavior Of The Elevation Prompt For Administrators | Prompt for consent on the secure desktop |
| User Account Control Behavior Of The Elevation Prompt For Standard Users | Prompt for credentials on the secure desktop |
| User Account Control Detect Application Installations And Prompt For Elevation | Enable |
| User Account Control Only Elevate UI Access Applications That Are Installed In Secure Locations | Enabled: Application runs with UIAccess integrity only if it resides in secure location. |
| User Account Control Run All Administrators In Admin Approval Mode | Enabled |
| User Account Control Switch To The Secure Desktop When Prompting For Elevation | Enabled |
| User Account Control Use Admin Approval Mode | Enable |
| User Account Control Virtualize File And Registry Write Failures To Per User Locations | Enabled |

Table 126. Settings - Win - Device Security - D - Local Security Policies - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 127. Assignments - Win - Device Security - D - Local Security Policies - v1.0.0

* + 1. Win - Device Security - D - Location and Privacy - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Location and Privacy - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:15 |
| Last modified | 10 April 2025 09:27:15 |
| Scope tags | Default |

Table 128. Basics - Win - Device Security - D - Location and Privacy - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Privacy | |
| Let Apps Access Location | User in control. |
| Let Apps Access Location Force Allow These Apps | windows.immersivecontrolpanel\_cw5n1h2txyewy;Microsoft.OutlookForWindows\_8wekyb3d8bbwe |
| System | |
| Allow Location | Location service is allowed. The user has control and can change Location Privacy settings on or off. |

Table 129. Settings - Win - Device Security - D - Location and Privacy - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 130. Assignments - Win - Device Security - D - Location and Privacy - v1.0.0

* + 1. Win - Device Security - D - Login and Lock Screen - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Login and Lock Screen - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:16 |
| Last modified | 10 April 2025 09:27:16 |
| Scope tags | Default |

Table 131. Basics - Win - Device Security - D - Login and Lock Screen - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Above Lock | |
| Allow Cortana Above Lock | Block |
| Allow Toasts | Block |
| Administrative Templates | |
| Personalization | |
| Prevent enabling lock screen camera | Enabled |
| Prevent enabling lock screen slide show | Enabled |
| Logon | |
| Turn off app notifications on the lock screen | Enabled |
| Credential User Interface | |
| Do not display the password reveal button | Enabled |
| Windows Logon Options | |
| Configure the mode of automatically signing in and locking last interactive user after a restart or cold boot | Enabled |
| Configure the mode of automatically signing in and locking last interactive user after a restart or cold boot (Device) | Enabled if BitLocker is on and not suspended |
| Sign-in and lock last interactive user automatically after a restart | Enabled |
| Authentication | |
| Allow Aad Password Reset | Allow |
| Privacy | |
| Let Apps Activate With Voice Above Lock | Force deny. Windows apps cannot be activated by voice while the screen is locked, and users cannot change it. |

Table 132. Settings - Win - Device Security - D - Login and Lock Screen - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 133. Assignments - Win - Device Security - D - Login and Lock Screen - v1.0.0

* + 1. Win - Device Security - D - Network List Manager - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Network List Manager - v1.0.0 |
| Description | Added - Ellis Barrett |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 25 June 2025 18:01:42 |
| Last modified | 25 June 2025 18:02:53 |
| Scope tags | Default |

Table 134. Basics - Win - Device Security - D - Network List Manager - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Network List Manager | |
| Allowed Tls Authentication Endpoints | https://ncsi.standrew.co.uk |
| Configured Tls Authentication Network Name | StAH\_Secure |

Table 135. Settings - Win - Device Security - D - Network List Manager - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 136. Assignments - Win - Device Security - D - Network List Manager - v1.0.0

* + 1. Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:17 |
| Last modified | 10 April 2025 09:27:17 |
| Scope tags | Default |

Table 137. Basics - Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Remote Procedure Call | |
| Enable RPC Endpoint Mapper Client Authentication | Enabled |
| Restrict Unauthenticated RPC clients | Enabled |
| RPC Runtime Unauthenticated Client Restriction to Apply: | Authenticated |
| Remote Desktop Connection Client | |
| Do not allow passwords to be saved | Enabled |
| Device and Resource Redirection | |
| Do not allow drive redirection | Enabled |
| Security | |
| Always prompt for password upon connection | Enabled |
| Require secure RPC communication | Enabled |
| Require use of specific security layer for remote (RDP) connections | Enabled |
| Security Layer (Device) | SSL |
| Require user authentication for remote connections by using Network Level Authentication | Enabled |
| Set client connection encryption level | Enabled |
| Encryption Level | High Level |

Table 138. Settings - Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 139. Assignments - Win - Device Security - D - Remote Desktop Services and RPC - v1.0.0

* + 1. Win - Device Security - D - Security Hardening - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Security Hardening - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:18 |
| Last modified | 11 April 2025 14:29:43 |
| Scope tags | Default |

Table 140. Basics - Win - Device Security - D - Security Hardening - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| MS Security Guide | |
| Apply UAC restrictions to local accounts on network logons | Enabled |
| Configure SMB v1 client driver | Enabled |
| Configure MrxSmb10 driver | Disable driver (recommended) |
| Configure SMB v1 server | Disabled |
| Enable Structured Exception Handling Overwrite Protection (SEHOP) | Enabled |
| WDigest Authentication (disabling may require KB2871997) | Disabled |
| MSS (Legacy) | |
| MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | Enabled |
| DisableIPSourceRoutingIPv6 (Device) | Highest protection, source routing is completely disabled |
| MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | Enabled |
| DisableIPSourceRouting (Device) | Highest protection, source routing is completely disabled |
| MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Disabled |
| MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | Enabled |
| MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | Enabled |
| ScreenSaverGracePeriod (Device) | 0 |
| Network Connections | |
| Prohibit installation and configuration of Network Bridge on your DNS domain network | Enabled |
| Require domain users to elevate when setting a network's location | Enabled |
| Windows Connection Manager | |
| Minimize the number of simultaneous connections to the Internet or a Windows Domain | Enabled |
| Minimize Policy Options (Device) | 0 = Allow simultaneous connections |
| Prohibit connection to non-domain networks when connected to domain authenticated network | Enabled |
| Printers | |
| Allow Print Spooler to accept client connections | Disabled |
| Limits print driver installation to Administrators | Enabled |
| Point and Print Restrictions | Enabled |
| Users can only point and print to machines in their forest (Device) | False |
| Users can only point and print to these servers: (Device) | True |
| When installing drivers for a new connection: (Device) | Show warning and elevation prompt |
| When updating drivers for an existing connection: (Device) | Show warning and elevation prompt |
| Credentials Delegation | |
| Encryption Oracle Remediation | Enabled |
| Protection Level: (Device) | Force Updated Clients |
| Remote host allows delegation of non-exportable credentials | Enabled |
| Early Launch Antimalware | |
| Boot-Start Driver Initialization Policy | Enabled |
| Choose the boot-start drivers that can be initialized: | Good, unknown and bad but critical |
| Internet Communication settings | |
| Turn off downloading of print drivers over HTTP | Enabled |
| Turn off Internet download for Web publishing and online ordering wizards | Enabled |
| Remote Assistance | |
| Configure Offer Remote Assistance | Disabled |
| Configure Solicited Remote Assistance | Disabled |
| AutoPlay Policies | |
| Disallow Autoplay for non-volume devices | Enabled |
| Set the default behavior for AutoRun | Enabled |
| Default AutoRun Behavior | Do not execute any autorun commands |
| Turn off Autoplay | Enabled |
| Turn off Autoplay on: | All drives |
| Credential User Interface | |
| Enumerate administrator accounts on elevation | Disabled |
| File Explorer | |
| Configure Windows Defender SmartScreen | Enabled |
| Pick one of the following settings: (Device) | Warn and prevent bypass |
| Turn off Data Execution Prevention for Explorer | Disabled |
| Turn off heap termination on corruption | Disabled |
| HomeGroup | |
| Prevent the computer from joining a homegroup | Enabled |
| Push To Install | |
| Turn off Push To Install service | Enabled |
| RSS Feeds | |
| Prevent downloading of enclosures | Enabled |
| Windows Error Reporting | |
| Disable Windows Error Reporting | Disabled |
| Windows PowerShell | |
| Turn on PowerShell Script Block Logging | Enabled |
| Log script block invocation start / stop events: | False |
| WinRM Client | |
| Allow Basic authentication | Disabled |
| Allow unencrypted traffic | Disabled |
| Disallow Digest authentication | Enabled |
| WinRM Service | |
| Allow Basic authentication | Disabled |
| Allow unencrypted traffic | Disabled |
| Disallow WinRM from storing RunAs credentials | Enabled |
| Connectivity | |
| Allow Phone PC Linking | Block |
| Data Protection | |
| Allow Direct Memory Access | Block |
| Experience | |
| Allow Cortana | Block |
| Allow Manual MDM Unenrollment | Block |
| Games | |
| Allow Advanced Gaming Services | Block |
| Kerberos | |
| PK Init Hash Algorithm Configuration | Enabled |
| PK Init Hash Algorithm SHA1 | Not Supported |
| PK Init Hash Algorithm SHA256 | Default |
| PK Init Hash Algorithm SHA384 | Default |
| PK Init Hash Algorithm SHA512 | Default |
| Lanman Workstation | |
| Enable Insecure Guest Logons | Disabled |
| Privacy | |
| Disable Privacy Experience | Enabled |
| Security | |
| Allow Add Provisioning Package | Block |
| Allow Remove Provisioning Package | Block |
| Require Retrieve Health Certificate On Boot | Required. |
| Settings | |
| Page Visibility List | hide:gaming-gamebar;gaming-gamedvr;gaming-broadcasting;gaming-gamemode;gaming-xboxnetworking |
| Sudo | |
| Enable Sudo | Sudo is disabled. |
| System Services | |
| Configure Xbox Accessory Management Service Startup Mode | Disabled |
| Configure Xbox Live Auth Manager Service Startup Mode | Disabled |
| Configure Xbox Live Game Save Service Startup Mode | Disabled |
| Configure Xbox Live Networking Service Startup Mode | Disabled |
| Task Scheduler | |
| Enable Xbox Game Save Task | Disabled |
| Wi-Fi Settings | |
| Allow Auto Connect To Wi Fi Sense Hotspots | Block |
| Allow Internet Sharing | Block |
| Windows Ink Workspace | |
| Allow Windows Ink Workspace | ink workspace is enabled (feature is turned on), but the user cannot access it above the lock screen. |
| Wireless Display | |
| Allow Projection From PC | Your PC can discover and project to other devices. |
| Allow Projection To PC | Projection to PC is not allowed. Always off and the user cannot enable it. |
| Require Pin For Pairing | Pairing ceremony for new devices will always require a PIN |

Table 141. Settings - Win - Device Security - D - Security Hardening - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 142. Assignments - Win - Device Security - D - Security Hardening - v1.0.0

* + 1. Win - Device Security - D - Timezone - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Timezone - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:18 |
| Last modified | 10 April 2025 09:27:18 |
| Scope tags | Default |

Table 143. Basics - Win - Device Security - D - Timezone - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Time Providers | |
| Configure Windows NTP Client | Enabled |
| EventLogFlags (Device) | 3 |
| NtpServer (Device) | time.windows.com |
| Type (Device) | AllSync |
| Enable Windows NTP Client | Enabled |
| User Rights | |
| Change Time Zone | \*S-1-5-19;\*S-1-5-32-544;\*S-1-5-32-545 |

Table 144. Settings - Win - Device Security - D - Timezone - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 145. Assignments - Win - Device Security - D - Timezone - v1.0.0

* + 1. Win - Device Security - D - User Rights - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - User Rights - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:19 |
| Last modified | 10 April 2025 09:27:19 |
| Scope tags | Default |

Table 146. Basics - Win - Device Security - D - User Rights - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| User Rights | |
| Access From Network | \*S-1-5-32-544;\*S-1-5-32-555 |
| Allow Local Log On | \*S-1-5-32-544;\*S-1-5-32-545 |
| Backup Files And Directories | \*S-1-5-32-544 |
| Change System Time | \*S-1-5-19;\*S-1-5-32-544 |
| Create Global Objects | \*S-1-5-6;\*S-1-5-19;\*S-1-5-20;\*S-1-5-32-544 |
| Create Page File | \*S-1-5-32-544 |
| Create Symbolic Links | \*S-1-5-32-544 |
| Debug Programs | \*S-1-5-32-544 |
| Deny Access From Network | \*S-1-2-0;\*S-1-5-32-546 |
| Deny Local Log On | \*S-1-5-32-546 |
| Deny Remote Desktop Services Log On | \*S-1-5-32-546 |
| Generate Security Audits | \*S-1-5-19;\*S-1-5-20 |
| Impersonate Client | \*S-1-5-6;\*S-1-5-19;\*S-1-5-20;\*S-1-5-32-544 |
| Increase Scheduling Priority | \*S-1-5-32-544;\*S-1-5-90 |
| Load Unload Device Drivers | \*S-1-5-32-544 |
| Manage Auditing And Security Log | \*S-1-5-32-544 |
| Manage Volume | \*S-1-5-32-544 |
| Modify Firmware Environment | \*S-1-5-32-544 |
| Profile Single Process | \*S-1-5-32-544 |
| Remote Shutdown | \*S-1-5-32-544 |
| Restore Files And Directories | \*S-1-5-32-544 |
| Take Ownership | \*S-1-5-32-544 |

Table 147. Settings - Win - Device Security - D - User Rights - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 148. Assignments - Win - Device Security - D - User Rights - v1.0.0

* + 1. Win - Device Security - D - Windows Package Manager - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Windows Package Manager - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:20 |
| Last modified | 10 April 2025 09:27:20 |
| Scope tags | Default |

Table 149. Basics - Win - Device Security - D - Windows Package Manager - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Desktop App Installer | |
| Enable App Installer Experimental Features | Disabled |
| Enable App Installer Hash Override | Disabled |
| Enable App Installer Local Manifest Files | Disabled |
| Enable App Installer ms-appinstaller protocol | Disabled |
| Enable App Installer Settings | Disabled |

Table 150. Settings - Win - Device Security - D - Windows Package Manager - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 151. Assignments - Win - Device Security - D - Windows Package Manager - v1.0.0

* + 1. Win - Device Security - D - Windows Subsystem for Linux - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - D - Windows Subsystem for Linux - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:22 |
| Last modified | 10 April 2025 09:27:22 |
| Scope tags | Default |

Table 152. Basics - Win - Device Security - D - Windows Subsystem for Linux - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Windows Subsystem For Linux | |
| Allow custom kernel configuration | Disabled |
| Allow custom networking configuration | Disabled |
| Allow custom system distribution configuration | Disabled |
| Allow kernel command line configuration | Disabled |
| Allow kernel debugging | Disabled |
| Allow nested virtualization | Disabled |
| Allow the debug shell | Disabled |
| Allow the Inbox version of the Windows Subsystem For Linux | Disabled |
| Allow user setting firewall configuration | Disabled |
| Allow WSL1 | Disabled |

Table 153. Settings - Win - Device Security - D - Windows Subsystem for Linux - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 154. Assignments - Win - Device Security - D - Windows Subsystem for Linux - v1.0.0

* + 1. Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0 |
| Description | WARNING: Applying this policy to Devices will cause a reboot between Device and User ESP phases!  NOTE: These features are automatically enabled on a fresh Win11 22H2 or above install, however they require Windows Enterprise to function correctly. They also require hardware support:  https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:22 |
| Last modified | 10 April 2025 09:27:22 |
| Scope tags | Default |

Table 155. Basics - Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Device Guard | |
| Configure System Guard Launch | Unmanaged Enables Secure Launch if supported by hardware |
| Credential Guard | (Enabled without lock) Turns on Credential Guard without UEFI lock. |
| Enable Virtualization Based Security | enable virtualization based security. |
| Machine Identity Isolation | (Disabled) Machine password is only LSASS-bound and stored in $MACHINE.ACC registry key. |
| Require Platform Security Features | Turns on VBS with Secure Boot and direct memory access (DMA). DMA requires hardware support. |
| Local Security Authority | |
| Configure Lsa Protected Process | Enabled without UEFI lock. LSA will run as protected process and this configuration is not UEFI locked. |
| Virtualization Based Technology | |
| Hypervisor Enforced Code Integrity | (Enabled without lock) Turns on Hypervisor-Protected Code Integrity without UEFI lock. |
| Require UEFI Memory Attributes Table | Require UEFI Memory Attributes Table |

Table 156. Settings - Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 157. Assignments - Win - Device Security - U - Device Guard, Credential Guard and HVCI - v1.0.0

* + 1. Win - Device Security - U - Power and Device Lock - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - U - Power and Device Lock - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:23 |
| Last modified | 10 April 2025 09:27:23 |
| Scope tags | Default |

Table 158. Basics - Win - Device Security - U - Power and Device Lock - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Sleep Settings | |
| Allow standby states (S1-S3) when sleeping (on battery) | Disabled |
| Allow standby states (S1-S3) when sleeping (plugged in) | Disabled |
| Require a password when a computer wakes (on battery) | Enabled |
| Require a password when a computer wakes (plugged in) | Enabled |
| Specify the system sleep timeout (on battery) | Enabled |
| System Sleep Timeout (seconds): | 600 |
| Specify the system sleep timeout (plugged in) | Enabled |
| System Sleep Timeout (seconds): | 900 |
| Video and Display Settings | |
| Turn off the display (on battery) | Enabled |
| On battery power, turn display off after (seconds) | 300 |
| Turn off the display (plugged in) | Enabled |
| When plugged in, turn display off after (seconds) | 600 |
| Shutdown | |
| Require use of fast startup | Disabled |
| Power | |
| Allow Hibernate | Block |
| Unattended Sleep Timeout On Battery | 600 |
| Unattended Sleep Timeout Plugged In | 900 |

Table 159. Settings - Win - Device Security - U - Power and Device Lock - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 160. Assignments - Win - Device Security - U - Power and Device Lock - v1.0.0

* + 1. Win - Device Security - U - Windows Sandbox - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Device Security - U - Windows Sandbox - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:24 |
| Last modified | 10 April 2025 09:27:24 |
| Scope tags | Default |

Table 161. Basics - Win - Device Security - U - Windows Sandbox - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Windows Sandbox | |
| Allow Audio Input | Not allowed. |
| Allow Clipboard Redirection | Allowed. |
| Allow Networking | Not allowed. |
| Allow Printer Redirection | Not allowed. |
| Allow VGPU | Not allowed. |
| Allow Video Input | Not allowed. |

Table 162. Settings - Win - Device Security - U - Windows Sandbox - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 163. Assignments - Win - Device Security - U - Windows Sandbox - v1.0.0

* + 1. Win - Dispensation - CIS -L1 - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Dispensation - CIS -L1 - D - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:25 |
| Last modified | 02 May 2025 12:38:45 |
| Scope tags | Default |

Table 164. Basics - Win - Dispensation - CIS -L1 - D - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Windows Connection Manager | |
| Minimize the number of simultaneous connections to the Internet or a Windows Domain | Enabled |
| Minimize Policy Options (Device) | 0 = Allow simultaneous connections |
| Mitigation Options | |
| Untrusted Font Blocking | Disabled |
| Local Policies Security Options | |
| Accounts Enable Administrator Account Status | Enable |
| Accounts Rename Administrator Account | "SupportDesk" |
| Interactive Logon Do Not Require CTRLALTDEL | Enabled (a user is not required to press CTRL+ALT+DEL to log on) |
| User Account Control Allow UI Access Applications To Prompt For Elevation | enabled (allow UIAccess applications to prompt for elevation without using the secure desktop) |
| User Account Control Behavior Of The Elevation Prompt For Standard Users | Prompt for credentials on the secure desktop |
| User Rights | |
| Access From Network | STANDREW\Domain Users |

Table 165. Settings - Win - Dispensation - CIS -L1 - D - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 166. Assignments - Win - Dispensation - CIS -L1 - D - v1.0.0

* + 1. Win - Dispensation - CIS -L1 - U - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Dispensation - CIS -L1 - U - v1.0.0 |
| Description | Settings for Interactive Logon Message, removed from Win - Dispensation - CIS -L1 - D - v1.0.0 as they will break Autopilot if deployed to Device. |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 17 April 2025 10:03:03 |
| Last modified | 17 April 2025 10:08:11 |
| Scope tags | Default |

Table 167. Basics - Win - Dispensation - CIS -L1 - U - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Local Policies Security Options | |
| Interactive Logon Message Text For Users Attempting To Log On | This computer system is the property of St Andrew’s Healthcare and is for use by authorised parties only.;Any use of this system, including all files accessed, may be intercepted, monitored, recorded and audited. Unauthorised or improper usage of this system, data or information may result in disciplinary action, sanction for third parties and/or criminal proceedings.;By clicking OK and logging on to this system, you agree to abide by the St Andrew’s Acceptable Use Standard which can be found on the Information Security Intranet site. |
| Interactive Logon Message Title For Users Attempting To Log On | "St Andrew's Healthcare" |

Table 168. Settings - Win - Dispensation - CIS -L1 - U - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 169. Assignments - Win - Dispensation - CIS -L1 - U - v1.0.0

* + 1. Win - Encryption - D - BitLocker (OS Disk) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Encryption - D - BitLocker (OS Disk) - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Disk encryption |
| Policy type | BitLocker |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:25 |
| Last modified | 17 June 2025 13:28:49 |
| Scope tags | Default |

Table 170. Basics - Win - Encryption - D - BitLocker (OS Disk) - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Operating System Drives | |
| Enforce drive encryption type on operating system drives | Enabled |
| Select the encryption type: (Device) | Full encryption |
| Require additional authentication at startup | Enabled |
| Configure TPM startup key and PIN: | Do not allow startup key and PIN with TPM |
| Configure TPM startup PIN: | Do not allow startup PIN with TPM |
| Configure TPM startup: | Require TPM |
| Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) | False |
| Configure TPM startup key: | Do not allow startup key with TPM |
| Disallow standard users from changing the PIN or password | Enabled |
| Choose how BitLocker-protected operating system drives can be recovered | Enabled |
| Omit recovery options from the BitLocker setup wizard | True |
| Allow data recovery agent | False |
|  | Allow 256-bit recovery key |
| Configure storage of BitLocker recovery information to AD DS: | Store recovery passwords and key packages |
| Do not enable BitLocker until recovery information is stored to AD DS for operating system drives | True |
| Save BitLocker recovery information to AD DS for operating system drives | True |
| Configure user storage of BitLocker recovery information: | Require 48-digit recovery password |
| BitLocker Drive Encryption | |
| Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later) | Enabled |
| Select the encryption method for removable data drives: | AES-CBC 256-bit |
| Select the encryption method for fixed data drives: | XTS-AES 256-bit |
| Select the encryption method for operating system drives: | XTS-AES 256-bit |
| BitLocker | |
| Require Device Encryption | Enabled |
| Allow Warning For Other Disk Encryption | Disabled |
| Allow Standard User Encryption | Enabled |
| Configure Recovery Password Rotation | Refresh on for Azure AD-joined devices |

Table 171. Settings - Win - Encryption - D - BitLocker (OS Disk) - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 172. Assignments - Win - Encryption - D - BitLocker (OS Disk) - v1.0.0

* + 1. Win - Health Monitoring - D - MDM wins over GPO - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Health Monitoring - D - MDM wins over GPO - v1.0.0 |
| Description | Sets MDM to win over GPO. |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:26 |
| Last modified | 10 April 2025 09:27:26 |
| Scope tags | Default |

Table 173. Basics - Win - Health Monitoring - D - MDM wins over GPO - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Control Policy Conflict | |
| MDM Wins Over GP | The MDM policy is used and the GP policy is blocked. |

Table 174. Settings - Win - Health Monitoring - D - MDM wins over GPO - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 175. Assignments - Win - Health Monitoring - D - MDM wins over GPO - v1.0.0

* + 1. Win - Health Monitoring - D - Windows Update for Business - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Health Monitoring - D - Windows Update for Business - v1.0.0 |
| Description | NOTE: Contains policies required for Windows Update for Business Reports. Further configuration required:  https://learn.microsoft.com/en-us/windows/deployment/update/wufb-reports-enable |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:26 |
| Last modified | 10 April 2025 09:27:26 |
| Scope tags | Default |

Table 176. Basics - Win - Health Monitoring - D - Windows Update for Business - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| System | |
| Allow device name to be sent in Windows diagnostic data | Allowed. |
| Allow Telemetry | Full |
| Configure Telemetry Opt In Change Notification | Disable telemetry change notifications. |
| Configure Telemetry Opt In Settings Ux | Disable Telemetry opt-in Settings. |
| Windows Update For Business | |
| Allow Temporary Enterprise Feature Control | Allowed |

Table 177. Settings - Win - Health Monitoring - D - Windows Update for Business - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 178. Assignments - Win - Health Monitoring - D - Windows Update for Business - v1.0.0

* + 1. Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0 |
| Description | Added - Ellis Barrett |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 23 June 2025 15:50:45 |
| Last modified | 25 June 2025 11:17:02 |
| Scope tags | Default |

Table 179. Basics - Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Compatibility View | |
| Use Policy List of Internet Explorer 7 sites | Enabled |
| List of sites (Device) | sap-pt;sap-ec;sap-pt.standrew.co.uk;sap-ec.standrew.co.uk |

Table 180. Settings - Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 181. Assignments - Win - Internet Explorer (Legacy) - D - Compatibility View - v1.0.0

* + 1. Win - Internet Explorer (Legacy) - D - Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Internet Explorer (Legacy) - D - Security - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:29 |
| Last modified | 10 April 2025 09:27:29 |
| Scope tags | Default |

Table 182. Basics - Win - Internet Explorer (Legacy) - D - Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Advanced Page | |
| Allow software to run or install even if the signature is invalid | Disabled |
| Check for server certificate revocation | Enabled |
| Check for signatures on downloaded programs | Enabled |
| Do not allow ActiveX controls to run in Protected Mode when Enhanced Protected Mode is enabled | Enabled |
| Turn off encryption support | Enabled |
| Secure Protocol combinations | Only use TLS 1.2 |
| Turn on 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows | Enabled |
| Turn on Enhanced Protected Mode | Enabled |
| Internet Control Panel | |
| Prevent ignoring certificate errors | Enabled |
| Internet Zone | |
| Access data sources across domains | Enabled |
| Access data sources across domains | Disable |
| Allow cut, copy or paste operations from the clipboard via script | Enabled |
| Allow paste operations via script | Disable |
| Allow drag and drop or copy and paste files | Enabled |
| Allow drag and drop or copy and paste files | Disable |
| Allow loading of XAML files | Enabled |
| XAML Files | Disable |
| Allow only approved domains to use ActiveX controls without prompt | Enabled |
| Only allow approved domains to use ActiveX controls without prompt | Enable |
| Allow only approved domains to use the TDC ActiveX control | Enabled |
| Only allow approved domains to use the TDC ActiveX control | Enable |
| Allow script-initiated windows without size or position constraints | Enabled |
| Allow script-initiated windows without size or position constraints | Disable |
| Allow scripting of Internet Explorer WebBrowser controls | Enabled |
| Internet Explorer web browser control | Disable |
| Allow scriptlets | Enabled |
| Scriptlets | Disable |
| Allow updates to status bar via script | Enabled |
| Status bar updates via script | Disable |
| Allow VBScript to run in Internet Explorer | Enabled |
| Allow VBScript to run in Internet Explorer | Disable |
| Automatic prompting for file downloads | Enabled |
| Automatic prompting for file downloads | Disable |
| Don't run antimalware programs against ActiveX controls | Enabled |
| Don't run antimalware programs against ActiveX controls | Disable |
| Download signed ActiveX controls | Enabled |
| Download signed ActiveX controls | Disable |
| Download unsigned ActiveX controls | Enabled |
| Download unsigned ActiveX controls | Disable |
| Enable dragging of content from different domains across windows | Enabled |
| Enable dragging of content from different domains across windows | Disable |
| Enable dragging of content from different domains within a window | Enabled |
| Enable dragging of content from different domains within a window | Disable |
| Include local path when user is uploading files to a server | Enabled |
| Include local directory path when uploading files to a server | Disable |
| Initialize and script ActiveX controls not marked as safe | Enabled |
| Initialize and script ActiveX controls not marked as safe | Disable |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Launching applications and files in an IFRAME | Enabled |
| Launching applications and files in an IFRAME | Disable |
| Logon options | Enabled |
| Logon options | Prompt for user name and password |
| Navigate windows and frames across different domains | Enabled |
| Navigate windows and frames across different domains | Disable |
| Run .NET Framework-reliant components not signed with Authenticode | Enabled |
| Run .NET Framework-reliant components not signed with Authenticode | Disable |
| Run .NET Framework-reliant components signed with Authenticode | Enabled |
| Run .NET Framework-reliant components signed with Authenticode | Disable |
| Show security warning for potentially unsafe files | Enabled |
| Launching programs and unsafe files | Prompt |
| Turn on Cross-Site Scripting Filter | Enabled |
| Turn on Cross-Site Scripting (XSS) Filter | Enable |
| Turn on Protected Mode | Enabled |
| Protected Mode | Enable |
| Turn on SmartScreen Filter scan | Enabled |
| Use SmartScreen Filter | Enable |
| Use Pop-up Blocker | Enabled |
| Use Pop-up Blocker | Enable |
| Userdata persistence | Enabled |
| Userdata persistence | Disable |
| Web sites in less privileged Web content zones can navigate into this zone | Enabled |
| Web sites in less privileged Web content zones can navigate into this zone | Disable |
| Security Page | |
| Intranet Sites: Include all network paths (UNCs) | Disabled |
| Turn on certificate address mismatch warning | Enabled |
| Intranet Zone | |
| Don't run antimalware programs against ActiveX controls | Enabled |
| Don't run antimalware programs against ActiveX controls | Disable |
| Initialize and script ActiveX controls not marked as safe | Enabled |
| Initialize and script ActiveX controls not marked as safe | Disable |
| Java permissions | Enabled |
| Java permissions | High safety |
| Local Machine Zone | |
| Don't run antimalware programs against ActiveX controls | Enabled |
| Don't run antimalware programs against ActiveX controls | Disable |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Locked-Down Internet Zone | |
| Turn on SmartScreen Filter scan | Enabled |
| Use SmartScreen Filter | Enable |
| Locked-Down Intranet Zone | |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Locked-Down Local Machine Zone | |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Locked-Down Restricted Sites Zone | |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Turn on SmartScreen Filter scan | Enabled |
| Use SmartScreen Filter | Enable |
| Locked-Down Trusted Sites Zone | |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Restricted Sites Zone | |
| Access data sources across domains | Enabled |
| Access data sources across domains | Disable |
| Allow active scripting | Enabled |
| Allow active scripting | Disable |
| Allow binary and script behaviors | Enabled |
| Allow Binary and Script Behaviors | Disable |
| Allow cut, copy or paste operations from the clipboard via script | Enabled |
| Allow paste operations via script | Disable |
| Allow drag and drop or copy and paste files | Enabled |
| Allow drag and drop or copy and paste files | Disable |
| Allow file downloads | Enabled |
| Allow file downloads | Disable |
| Allow loading of XAML files | Enabled |
| XAML Files | Disable |
| Allow META REFRESH | Enabled |
| Allow META REFRESH | Disable |
| Allow only approved domains to use ActiveX controls without prompt | Enabled |
| Only allow approved domains to use ActiveX controls without prompt | Enable |
| Allow only approved domains to use the TDC ActiveX control | Enabled |
| Only allow approved domains to use the TDC ActiveX control | Enable |
| Allow script-initiated windows without size or position constraints | Enabled |
| Allow script-initiated windows without size or position constraints | Disable |
| Allow scripting of Internet Explorer WebBrowser controls | Enabled |
| Internet Explorer web browser control | Disable |
| Allow scriptlets | Enabled |
| Scriptlets | Disable |
| Allow updates to status bar via script | Enabled |
| Status bar updates via script | Disable |
| Allow VBScript to run in Internet Explorer | Enabled |
| Allow VBScript to run in Internet Explorer | Disable |
| Automatic prompting for file downloads | Enabled |
| Automatic prompting for file downloads | Disable |
| Don't run antimalware programs against ActiveX controls | Enabled |
| Don't run antimalware programs against ActiveX controls | Disable |
| Download signed ActiveX controls | Enabled |
| Download signed ActiveX controls | Disable |
| Download unsigned ActiveX controls | Enabled |
| Download unsigned ActiveX controls | Disable |
| Enable dragging of content from different domains across windows | Enabled |
| Enable dragging of content from different domains across windows | Disable |
| Enable dragging of content from different domains within a window | Enabled |
| Enable dragging of content from different domains within a window | Disable |
| Enable MIME Sniffing | Enabled |
| Enable MIME Sniffing | Disable |
| Include local path when user is uploading files to a server | Enabled |
| Include local directory path when uploading files to a server | Disable |
| Initialize and script ActiveX controls not marked as safe | Enabled |
| Initialize and script ActiveX controls not marked as safe | Disable |
| Java permissions | Enabled |
| Java permissions | Disable Java |
| Launching applications and files in an IFRAME | Enabled |
| Launching applications and files in an IFRAME | Disable |
| Logon options | Enabled |
| Logon options | Anonymous logon |
| Navigate windows and frames across different domains | Enabled |
| Navigate windows and frames across different domains | Disable |
| Run .NET Framework-reliant components not signed with Authenticode | Enabled |
| Run .NET Framework-reliant components not signed with Authenticode | Disable |
| Run .NET Framework-reliant components signed with Authenticode | Enabled |
| Run .NET Framework-reliant components signed with Authenticode | Disable |
| Run ActiveX controls and plugins | Enabled |
| Run ActiveX controls and plugins | Disable |
| Script ActiveX controls marked safe for scripting | Enabled |
| Script ActiveX controls marked safe for scripting | Disable |
| Scripting of Java applets | Enabled |
| Scripting of Java applets | Disable |
| Show security warning for potentially unsafe files | Enabled |
| Launching programs and unsafe files | Disable |
| Turn on Cross-Site Scripting Filter | Enabled |
| Turn on Cross-Site Scripting (XSS) Filter | Enable |
| Turn on Protected Mode | Enabled |
| Protected Mode | Enable |
| Turn on SmartScreen Filter scan | Enabled |
| Use SmartScreen Filter | Enable |
| Use Pop-up Blocker | Enabled |
| Use Pop-up Blocker | Enable |
| Userdata persistence | Enabled |
| Userdata persistence | Disable |
| Web sites in less privileged Web content zones can navigate into this zone | Enabled |
| Web sites in less privileged Web content zones can navigate into this zone | Disable |
| Trusted Sites Zone | |
| Don't run antimalware programs against ActiveX controls | Enabled |
| Don't run antimalware programs against ActiveX controls | Disable |
| Initialize and script ActiveX controls not marked as safe | Enabled |
| Initialize and script ActiveX controls not marked as safe | Disable |
| Java permissions | Enabled |
| Java permissions | High safety |
| Internet Explorer | |
| Prevent bypassing SmartScreen Filter warnings | Enabled |
| Prevent bypassing SmartScreen Filter warnings about files that are not commonly downloaded from the Internet | Disabled |
| Prevent managing SmartScreen Filter | Enabled |
| Select SmartScreen Filter mode | On |
| Prevent per-user installation of ActiveX controls | Enabled |
| Security Zones: Do not allow users to add/delete sites | Enabled |
| Security Zones: Do not allow users to change policies | Enabled |
| Security Zones: Use only machine settings | Enabled |
| Specify use of ActiveX Installer Service for installation of ActiveX controls | Enabled |
| Turn off Crash Detection | Enabled |
| Turn off the Security Settings Check feature | Disabled |
| Turn on the auto-complete feature for user names and passwords on forms (User) | Disabled |
| Add-on Management | |
| Remove "Run this time" button for outdated ActiveX controls in Internet Explorer | Enabled |
| Turn off blocking of outdated ActiveX controls for Internet Explorer | Disabled |
| Security Features | |
| Allow fallback to SSL 3.0 (Internet Explorer) | Enabled |
| Allow insecure fallback for: | No Sites |
| Consistent Mime Handling | |
| Internet Explorer Processes | Enabled |
| Mime Sniffing Safety Feature | |
| Internet Explorer Processes | Enabled |
| MK Protocol Security Restriction | |
| Internet Explorer Processes | Enabled |
| Notification bar | |
| Internet Explorer Processes | Enabled |
| Protection From Zone Elevation | |
| Internet Explorer Processes | Enabled |
| Restrict ActiveX Install | |
| Internet Explorer Processes | Enabled |
| Restrict File Download | |
| Internet Explorer Processes | Enabled |
| Scripted Window Security Restrictions | |
| Internet Explorer Processes | Enabled |

Table 183. Settings - Win - Internet Explorer (Legacy) - D - Security - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 184. Assignments - Win - Internet Explorer (Legacy) - D - Security - v1.0.0

* + 1. Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0 |
| Description | Added - Ellis Barrett |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 23 June 2025 16:36:01 |
| Last modified | 25 June 2025 17:28:48 |
| Scope tags | Default |

Table 185. Basics - Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Security Page | |
| Site to Zone Assignment List | Enabled |
| Name | \*.simplysign.co.uk |
| Value | 2 |
| Name | \*.natwestbusinesscard.com |
| Value | 2 |
| Name | \*.medefinance.com |
| Value | 2 |
| Name | web.signlive.com |
| Value | 2 |
| Name | support.agresso.com |
| Value | 2 |
| Name | stahstah.app.box.com |
| Value | 2 |
| Name | tfs |
| Value | 2 |
| Name | sahcorp.sharepoint.com |
| Value | 2 |
| Name | riotrain |
| Value | 2 |
| Name | rio7 |
| Value | 2 |
| Name | rio-train |
| Value | 2 |
| Name | rio |
| Value | 2 |
| Name | iar.standrew.arcusglobal.com |
| Value | 2 |
| Name | \*.gateway.gov.uk |
| Value | 2 |
| Name | crc.environment-agency.gov.uk |
| Value | 2 |
| Name | consultancy |
| Value | 2 |
| Name | \*.bright-cloud.net |
| Value | 2 |
| Name | \*.beagle.psl-uk.co.uk |
| Value | 2 |
| Name | agressoliveweb |
| Value | 2 |
| Name | \*.zoopla.co.uk |
| Value | 2 |
| Name | \*.website.com |
| Value | 2 |
| Name | \*.voca.com |
| Value | 2 |
| Name | \*.uk-plc.net |
| Value | 2 |
| Name | \*.tradeonlineservices.com |
| Value | 2 |
| Name | \*.successfactors.eu |
| Value | 2 |
| Name | \*.successfactors.com |
| Value | 2 |
| Name | \*.standrew.micadipr.net |
| Value | 2 |
| Name | \*.standrew.co.uk |
| Value | 2 |
| Name | \*.sapsf.eu |
| Value | 2 |
| Name | \*.sapoci.cityelectricalfactors.co.uk |
| Value | 2 |
| Name | \*.sapjam.com |
| Value | 2 |
| Name | \*.sap.com |
| Value | 2 |
| Name | \*.plateau.com |
| Value | 2 |
| Name | \*.ondemand.com |
| Value | 2 |
| Name | \*.lyreco.com |
| Value | 2 |
| Name | \*.lyreco.co.uk |
| Value | 2 |
| Name | \*.lloydsbank.com |
| Value | 2 |
| Name | \*.launch.choota.com |
| Value | 2 |
| Name | \*.gopas.cz |
| Value | 2 |
| Name | \*.globalrispacs.com |
| Value | 2 |
| Name | \*.fpsdca.co.uk |
| Value | 2 |
| Name | \*.fileopen.com |
| Value | 2 |
| Name | \*.nhs.uk |
| Value | 2 |
| Name | \*.dashlane.com |
| Value | 2 |
| Name | \*.course-source.net |
| Value | 2 |
| Name | \*.coremotives.com |
| Value | 2 |
| Name | \*.cloudbuy.com |
| Value | 2 |
| Name | \*.boldchat.com |
| Value | 2 |
| Name | \*.bold360.com |
| Value | 2 |
| Name | \*.blackwells.co.uk |
| Value | 2 |
| Name | \*.blackwell.co.uk |
| Value | 2 |
| Name | \*.barclayswealth.com |
| Value | 2 |
| Name | \*.barclays.net |
| Value | 2 |
| Name | \*.barclays.com |
| Value | 2 |
| Name | \*.bacs.co.uk |
| Value | 2 |
| Name | \*.atlassian.net |
| Value | 2 |
| Name | \*.atlassian.com |
| Value | 2 |
| Name | \*.arco.co.uk |
| Value | 2 |
| Name | stah |
| Value | 1 |
| Name | nn-dwdb-11 |
| Value | 1 |
| Name | 10.20.26.200 |
| Value | 1 |
| Name | nn-infsql12-02 |
| Value | 2 |
| Name | v-nn-apps-11 |
| Value | 2 |
| Name | v-nn-erpec-21 |
| Value | 2 |
| Name | v-nn-erppt-21 |
| Value | 2 |
| Name | v-nn-erppt-31 |
| Value | 2 |

Table 186. Settings - Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 187. Assignments - Win - Internet Explorer (Legacy) - D - Zone Assignment - v1.0.0

* + 1. Win - MDE - D - Onboarding - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - MDE - D - Onboarding - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | EndpointDetectionAndResponse |
| Policy type | Endpoint detection and response |
| Platform supported | Windows 10 and later |
| Created | 11 April 2025 14:20:22 |
| Last modified | 17 June 2025 13:26:54 |
| Scope tags | Default |

Table 188. Basics - Win - MDE - D - Onboarding - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Defender for Endpoint | |
| Microsoft Defender for Endpoint client configuration package type | Auto from connector |
| Onboarding blob from Connector | f12f59c6-12e3-4087-b592-aafc4f22820e |
| Sample Sharing | All |

Table 189. Settings - Win - MDE - D - Onboarding - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 190. Assignments - Win - MDE - D - Onboarding - v1.0.0

* + 1. Win - Microsoft Accounts - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Accounts - D - Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:30 |
| Last modified | 10 April 2025 09:27:30 |
| Scope tags | Default |

Table 191. Basics - Win - Microsoft Accounts - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Accounts | |
| Allow Adding Non Microsoft Accounts Manually | Block |
| Allow Microsoft Account Connection | Block |
| Administrative Templates | |
| App runtime | |
| Allow Microsoft accounts to be optional | Enabled |
| Microsoft account | |
| Block all consumer Microsoft account user authentication | Enabled |
| Local Policies Security Options | |
| Accounts Block Microsoft Accounts | Users can't add or log on with Microsoft accounts |

Table 192. Settings - Win - Microsoft Accounts - D - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 193. Assignments - Win - Microsoft Accounts - D - Configuration - v1.0.0

* + 1. Win - Microsoft Edge - D - Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - D - Security - v1.0.0 |
| Description | Updated - Ellis Barrett  Allow pop-up windows on specific sites  Allow Cookies on specific sites |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:31 |
| Last modified | 25 June 2025 11:17:40 |
| Scope tags | Default |

Table 194. Basics - Win - Microsoft Edge - D - Security - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Ads setting for sites with intrusive ads | Enabled |
| Ads setting for sites with intrusive ads (Device) | Block ads on sites with intrusive ads. (Default value) |
| Allow download restrictions | Enabled |
| Download restrictions (Device) | Block malicious downloads and dangerous file types |
| Allow importing of browser settings | Disabled |
| Allow importing of browsing history | Disabled |
| Allow importing of home page settings | Disabled |
| Allow importing of payment info | Disabled |
| Allow importing of saved passwords | Disabled |
| Allow importing of search engine settings | Disabled |
| Allow managed extensions to use the Enterprise Hardware Platform API | Disabled |
| Allow personalization of ads, search and news by sending browsing history to Microsoft | Disabled |
| Allow queries to a Browser Network Time service | Enabled |
| Allow the Search bar at Windows startup (obsolete) | Disabled |
| Allow users to proceed from the HTTPS warning page | Disabled |
| Allow websites to query for available payment methods | Disabled |
| Block tracking of users' web-browsing activity | Enabled |
| Block tracking of users' web-browsing activity (Device) | Balanced (blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized) |
| Clear browsing data when Microsoft Edge closes | Disabled |
| Clear cached images and files when Microsoft Edge closes | Disabled |
| Configure the Share experience | Disabled |
| Control communication with the Experimentation and Configuration Service | Enabled |
| Control communication with the Experimentation and Configuration Service (Device) | Disable communication with the Experimentation and Configuration Service |
| DNS interception checks enabled | Enabled |
| Enable AutoFill for addresses | Disabled |
| Enable AutoFill for payment instruments | Disabled |
| Enable renderer code integrity (deprecated) | Enabled |
| Hide the First-run experience and splash screen | Enabled |
| Microsoft Edge Insider Promotion Enabled | Disabled |
| Minimum TLS version enabled | Enabled |
| Minimum SSL version enabled (Device) | TLS 1.2 |
| Cast | |
| Enable Google Cast | Disabled |
| Content settings | |
| Allow cookies on specific sites | Enabled |
| Allow cookies on specific sites (Device) | [\*.]plateau.com;hcm12preview.sapsf.eu |
| Allow pop-up windows on specific sites | Enabled |
| Allow pop-up windows on specific sites (Device) | consultany;rio;[\*.]plateau.com;hcm12preview.sapsf.eu;[\*.]standrew.co.uk |
| Experimentation | |
| Configure users ability to override feature flags | Disabled |
| HTTP authentication | |
| Supported authentication schemes | Enabled |
| Supported authentication schemes (Device) | ntlm,negotiate |
| Windows Hello For HTTP Auth Enabled | Enabled |
| Native Messaging | |
| Allow user-level native messaging hosts (installed without admin permissions) | Disabled |
| SmartScreen settings | |
| Configure Microsoft Defender SmartScreen | Enabled |
| Configure Microsoft Defender SmartScreen to block potentially unwanted apps | Enabled |
| Force Microsoft Defender SmartScreen checks on downloads from trusted sources | Enabled |
| Prevent bypassing Microsoft Defender SmartScreen prompts for sites | Enabled |
| Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads | Enabled |
| Typosquatting Checker settings | |
| Configure Edge Website Typo Protection | Enabled |

Table 195. Settings - Win - Microsoft Edge - D - Security - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 196. Assignments - Win - Microsoft Edge - D - Security - v1.0.0

* + 1. Win - Microsoft Edge - U - Extensions - v1.1.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - U - Extensions - v1.1.0 |
| Description | Cloned policy from Win - Microsoft Edge - U - Extensions - v1.0.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 07 July 2025 15:06:21 |
| Last modified | 07 July 2025 15:53:10 |
| Scope tags | Default |

Table 197. Basics - Win - Microsoft Edge - U - Extensions - v1.1.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Extensions | |
| Allow specific extensions to be installed (User) | Enabled |
| Extension IDs to exempt from the block list (User) | dppgmdbiimibapkepcbdbmkaabgiofem;bpgncafocbpieaeigfcookhgmeamglgo;https://clients2.google.com/service/update2/crx;ofefcgjbeghpigppfmkologfjadafddi;nkbndigcebkoaejohleckhekfmcecfja |
| Blocks external extensions from being installed (User) | Enabled |
| Control which extensions are installed silently (User) | Enabled |
| Extension/App IDs and update URLs to be silently installed (User) | nkbndigcebkoaejohleckhekfmcecfja;ofefcgjbeghpigppfmkologfjadafddi;bpgncafocbpieaeigfcookhgmeamglgo;https://clients2.google.com/service/update2/crx |
| Control which extensions cannot be installed (User) | Enabled |
| Extension IDs the user should be prevented from installing (or \* for all) (User) | \* |

Table 198. Settings - Win - Microsoft Edge - U - Extensions - v1.1.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 199. Assignments - Win - Microsoft Edge - U - Extensions - v1.1.0

* + 1. Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:32 |
| Last modified | 16 May 2025 16:10:01 |
| Scope tags | Default |

Table 200. Basics - Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Browser | |
| Configure Home Button | Show home button and load the Start page |
| Home Pages | https://sahcorp.sharepoint.com/sites/theHub |
| Set Home Button URL | https://sahcorp.sharepoint.com/sites/theHub |
| Set New Tab Page URL | https://sahcorp.sharepoint.com/sites/theHub |
| Microsoft Edge | |
| Configure favorites | Enabled |
| Configure favorites (Device) | [{"toplevel\_name":"StAH Favourites"},{"name":"St Andrews Clinical Links","children":[{"name":"MICAD","url":"https://standrew-cp.micadhd.net/default.aspx"},{"name":"RIO","url":"https://rio/rio/login/riologinsrc.asp?database=LIVE&imp=1"},{"name":"Loop","url":"https://web.loop.allocate-cloud.co.uk/loop/login"},{"name":"Datix","url":"https://datix/datix/live/"},{"name":"Trauma Response","url":"https://sahcorp.sharepoint.com/sites/stahTRS"},{"name":"First Aid Responders","url":"https://sahcorp.sharepoint.com/sites/HRServices/First%20Aid%20Responder%20List/Forms/AllItems.aspx"},{"name":"Clinical Supervision","url":"https://apps.powerapps.com/play/e/3cdd4913-a073-423e-a781-64f7f8904d63/a/fdf02275-e304-4ad6-a4b9-749e942271c6?tenantId=e2247d94-9c54-40ae-98ad-6ce6ba7bcbad"},{"name":"Infection Prevention","url":"https://www.england.nhs.uk/publication/national-infection-prevention-and-control/"},{"name":"Gift & Hospitality","url":"https://sahcorp.sharepoint.com/sites/stahGovernance/Lists/Gift%20and%20Hospitality%20Register"},{"name":"24hr Staff Counselling","url":"https://sahcorp.sharepoint.com/sites/stahHEAP"},{"name":"My IT","url":"https://myit.stah.org/stah"},{"name":"Health Roster","url":"https://stah.allocate-cloud.co.uk/HealthRoster/STAHLIVE/"},{"name":"SAP Self-Service","url":"https://sap-pt.standrew.co.uk/irj/portal"}]}] |
| Startup, home page and new tab page | |
| Action to take on Microsoft Edge startup | Enabled |
| Action to take on startup (Device) | Open a new tab |
| Configure the home page URL | Enabled |
| Home page URL (Device) | https://sahcorp.sharepoint.com/sites/theHub |
| Configure the Microsoft Edge new tab page experience | Enabled |
| New tab page experience (Device) | Microsoft News feed experience |
| Configure the new tab page URL | Enabled |
| New tab page URL (Device) | https://sahcorp.sharepoint.com/sites/theHub |
| Set the new tab page as the home page | Enabled |
| Show Home button on toolbar | Enabled |
| Sites to open when the browser starts | Enabled |
| Sites to open when the browser starts (Device) | https://sahcorp.sharepoint.com/sites/theHub |

Table 201. Settings - Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 202. Assignments - Win - Microsoft Edge - U - Homepage and Bookmarks - v1.0.0

* + 1. Win - Microsoft Edge - U - Password Management - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - U - Password Management - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:32 |
| Last modified | 10 April 2025 09:27:32 |
| Scope tags | Default |

Table 203. Basics - Win - Microsoft Edge - U - Password Management - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Password manager and protection | |
| Allow users to be alerted if their passwords are found to be unsafe (User) | Enabled |
| Allow users to get a strong password suggestion whenever they are creating an account online (User) | Enabled |
| Configures a setting that asks users to enter their device password while using password autofill (User) | Enabled |
| Configures a setting that asks users to enter their device password while using password autofill (User) | With device password |
| Enable saving passwords to the password manager (User) | Enabled |

Table 204. Settings - Win - Microsoft Edge - U - Password Management - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 205. Assignments - Win - Microsoft Edge - U - Password Management - v1.0.0

* + 1. Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0 |
| Description | Enable profile creation from the Identity flyout menu or the Settings page (User) set to Enable on 10.06.25 by PC |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:33 |
| Last modified | 10 June 2025 12:14:35 |
| Scope tags | Default |

Table 206. Basics - Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Automatically import another browser's data and settings at first run (User) | Disabled |
| Browser sign-in settings (User) | Enabled |
| Browser sign-in settings (User) | Force users to sign-in to use the browser |
| Configure whether a user always has a default profile automatically signed in with their work or school account (User) | Enabled |
| Enable profile creation from the Identity flyout menu or the Settings page (User) | Enabled |
| Enable use of ephemeral profiles (User) | Disabled |
| Force synchronization of browser data and do not show the sync consent prompt (User) | Enabled |
| Single sign-on for work or school sites using this profile enabled (User) | Enabled |
| Identity and sign-in | |
| Enable implicit sign-in (User) | Enabled |

Table 207. Settings - Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 208. Assignments - Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v1.0.0

* + 1. Win - Microsoft Edge - U - User Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Edge - U - User Experience - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:33 |
| Last modified | 10 April 2025 09:27:33 |
| Scope tags | Default |

Table 209. Basics - Win - Microsoft Edge - U - User Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Allow users to access the games menu (User) | Disabled |
| Enable CryptoWallet feature (obsolete) (User) | Disabled |
| Enable full-tab promotional content (deprecated) (User) | Disabled |
| Microsoft Edge built-in PDF reader powered by Adobe Acrobat enabled (User) | Enabled |
| Shopping in Microsoft Edge Enabled (User) | Disabled |
| Show Microsoft Rewards experiences (User) | Disabled |
| Shows button on native PDF viewer in Microsoft Edge that allows users to sign up for Adobe Acrobat subscription (User) | Disabled |
| Edge Workspaces settings | |
| Enable Workspaces (User) | Enabled |
| Microsoft Edge - Default Settings (users can override) | |
| Performance | |
| Enable startup boost (User) | Disabled |
| Sleeping Tabs settings | |
| Configure Sleeping Tabs (User) | Enabled |
| Startup, home page and new tab page | |
| Action to take on Microsoft Edge startup (User) | Enabled |
| Action to take on startup (User) | Restore the last session |
| Configure the Microsoft Edge new tab page experience (User) | Enabled |
| New tab page experience (User) | Office 365 feed experience |
| Set new tab page quick links (User) | Disabled |
| Show Home button on toolbar (User) | Enabled |

Table 210. Settings - Win - Microsoft Edge - U - User Experience - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 211. Assignments - Win - Microsoft Edge - U - User Experience - v1.0.0

* + 1. Win - Microsoft Office - U - Config and Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Office - U - Config and Experience - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:35 |
| Last modified | 10 April 2025 09:27:35 |
| Scope tags | Default |

Table 212. Basics - Win - Microsoft Office - U - Config and Experience - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Excel 2016 | |
| Save | |
| Default file format (User) | Enabled |
| Save Excel files as (User) | Excel Workbook (\*.xlsx) |
| Suppress file format compatibility dialog box for OpenDocument Spreadsheet format (User) | Enabled |
| Microsoft Office 2016 | |
| First Run | |
| Disable First Run Movie (User) | Enabled |
| Disable Office First Run on application boot (User) | Enabled |
| Display Language | |
| Allow users who aren’t admins to install language accessory packs (User) | Enabled |
| Language Preferences | |
| Notify users if they do not have proofing tools for a language they use (User) | Enabled |
| Miscellaneous | |
| File links open preference default selection as Desktop App (User) | Enabled |
| Hide Microsoft cloud-based file locations in the Backstage view (User) | Enabled |
| Online Storage Filter Value: (User) | 137 |
| Suppress recommended settings dialog (User) | Enabled |
| Trust Center | |
| Allow users to receive and respond to in-product surveys from Microsoft (User) | Disabled |
| [Deprecated] Allow users to receive and respond to in-product surveys from Microsoft (User) | Disabled |
| Disable Opt-in Wizard on first run (User) | Enabled |
| Enable Customer Experience Improvement Program (User) | Disabled |
| Microsoft Outlook 2016 | |
| Exchange | |
| Automatically configure profile based on Active Directory Primary SMTP address (User) | Enabled |
| Prefer the provided account email in AutoDiscover auth prompts. (User) | Enabled |
| Prevent adding non-default Exchange accounts (User) | Enabled |
| Cached Exchange Mode | |
| Download shared non-mail folders (User) | Disabled |
| Use Cached Exchange Mode for new and existing Outlook profiles (User) | Enabled |
| Use the Online Global Address List for Nickname Resolution (User) | Enabled |
| RSS Feeds | |
| Turn off RSS feature (User) | Enabled |
| Other | |
| Disable Outlook Mobile Hyperlink (User) | Enabled |
| Make Outlook the default program for E-mail, Contacts, and Calendar (User) | Enabled |
| Microsoft PowerPoint 2016 | |
| Save | |
| Default file format (User) | Enabled |
| Save PowerPoint files as (User) | PowerPoint Presentation (\*.pptx) |
| Suppress file format compatibility dialog box for OpenDocument Presentation format (User) | Enabled |
| Microsoft Word 2016 | |
| Save | |
| Default file format (User) | Enabled |
| Save Word files as (User) | Word Document (\*.docx) |
| Do not display file format compatibility dialog box for OpenDocument text format (User) | Enabled |

Table 213. Settings - Win - Microsoft Office - U - Config and Experience - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 214. Assignments - Win - Microsoft Office - U - Config and Experience - v1.0.0

* + 1. Win - Microsoft Office - U - Macros - ALLOW - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Office - U - Macros - ALLOW - v1.0.0 |
| Description | Cloned policy from Win - Microsoft Office - U - Macros - BLOCK - v1.0.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 19 June 2025 10:04:03 |
| Last modified | 19 June 2025 10:04:59 |
| Scope tags | Default |

Table 215. Basics - Win - Microsoft Office - U - Macros - ALLOW - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Access 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft Excel 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft PowerPoint 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft Project 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft Publisher 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft Visio 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |
| Microsoft Word 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Enable all macros (not recommended) |

Table 216. Settings - Win - Microsoft Office - U - Macros - ALLOW - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Windows-Office-MacrosAllowed | \*StAH-Win-Filter-Baseline - All | Include |

Table 217. Assignments - Win - Microsoft Office - U - Macros - ALLOW - v1.0.0

* + 1. Win - Microsoft Office - U - Macros - BLOCK - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Office - U - Macros - BLOCK - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:34 |
| Last modified | 18 June 2025 14:42:09 |
| Scope tags | Default |

Table 218. Basics - Win - Microsoft Office - U - Macros - BLOCK - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Access 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft Excel 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft PowerPoint 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft Project 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft Publisher 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft Visio 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |
| Microsoft Word 2016 | |
| Trust Center | |
| VBA Macro Notification Settings (User) | Enabled |
|  | Disable all without notification |

Table 219. Settings - Win - Microsoft Office - U - Macros - BLOCK - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |
| Excluded Groups | | |
| Intune-Windows-Office-MacrosAllowed |  |  |

Table 220. Assignments - Win - Microsoft Office - U - Macros - BLOCK - v1.0.0

* + 1. Win - Microsoft OneDrive - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft OneDrive - D - Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:38 |
| Last modified | 23 April 2025 13:17:17 |
| Scope tags | Default |

Table 221. Basics - Win - Microsoft OneDrive - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OneDrive | |
| Allow syncing OneDrive accounts for only specific organizations | Enabled |
| Tenant ID: (Device) | e2247d94-9c54-40ae-98ad-6ce6ba7bcbad |
| Allow users to contact Microsoft for feedback and support | Disabled |
| Enable automatic upload bandwidth management for OneDrive | Enabled |
| Enable sync health reporting for OneDrive | Enabled |
| Exclude specific kinds of files from being uploaded | Enabled |
| Keywords: (Device) | \*.accdb;\*.appx;\*.bat;\*.cmd;\*.exe;\*.img;\*.iso;\*.jar;\*.lnk;\*.mdb;\*.msi;\*.pst;\*.reg;\*.vbs;\*.vhd;\*.vhdx;\*.vmdk |
| Prevent users from redirecting their Windows known folders to their PC | Enabled |
| Set the sync app update ring | Enabled |
| Update ring: (Device) | Production |
| Silently move Windows known folders to OneDrive | Enabled |
| Desktop (Device) | True |
| Documents (Device) | True |
| Pictures (Device) | True |
| Show notification to users after folders have been redirected: (Device) | Yes |
| Tenant ID: (Device) | e2247d94-9c54-40ae-98ad-6ce6ba7bcbad |
| Silently sign in users to the OneDrive sync app with their Windows credentials | Enabled |
| Use OneDrive Files On-Demand | Enabled |

Table 222. Settings - Win - Microsoft OneDrive - D - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 223. Assignments - Win - Microsoft OneDrive - D - Configuration - v1.0.0

* + 1. Win - Microsoft OneDrive - U - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft OneDrive - U - Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:39 |
| Last modified | 10 April 2025 09:27:39 |
| Scope tags | Default |

Table 224. Basics - Win - Microsoft OneDrive - U - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OneDrive | |
| Allow users to choose how to handle Office file sync conflicts (User) | Enabled |
| Disable the tutorial that appears at the end of OneDrive Setup (User) | Enabled |
| Prevent users from changing the location of their OneDrive folder (User) | Enabled |
| Name | e2247d94-9c54-40ae-98ad-6ce6ba7bcbad |
| Value | 1 |
| Prevent users from syncing personal OneDrive accounts (User) | Enabled |

Table 225. Settings - Win - Microsoft OneDrive - U - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 226. Assignments - Win - Microsoft OneDrive - U - Configuration - v1.0.0

* + 1. Win - Microsoft Store - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Store - D - Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:39 |
| Last modified | 10 April 2025 09:27:39 |
| Scope tags | Default |

Table 227. Basics - Win - Microsoft Store - D - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft App Store | |
| Allow All Trusted Apps | Explicit deny. |
| Allow apps from the Microsoft app store to auto update | Allowed. |
| Allow Developer Unlock | Explicit deny. |
| Allow Game DVR | Block |
| Block Non Admin User Install | Block |
| MSI Allow User Control Over Install | Disabled |
| MSI Always Install With Elevated Privileges | Disabled |

Table 228. Settings - Win - Microsoft Store - D - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 229. Assignments - Win - Microsoft Store - D - Configuration - v1.0.0

* + 1. Win - Microsoft Store - U - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Microsoft Store - U - Configuration - v1.0.0 |
| Description | NOTE: The "Turn off the Store application" setting does not work on Windows Pro/Business SKU's:  https://learn.microsoft.com/en-gb/windows/client-management/mdm/policy-csp-admx-windowsstore?WT.mc\_id=Portal-fx#removewindowsstore\_2 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:40 |
| Last modified | 10 April 2025 09:27:40 |
| Scope tags | Default |

Table 230. Basics - Win - Microsoft Store - U - Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Start Menu and Taskbar | |
| Do not allow pinning Store app to the Taskbar (User) | Enabled |
| Store | |
| Turn off the Store application (User) | Enabled |
| Microsoft App Store | |
| MSI Always Install With Elevated Privileges (User) | Disabled |
| Require Private Store Only | Only Private store is enabled. |

Table 231. Settings - Win - Microsoft Store - U - Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 232. Assignments - Win - Microsoft Store - U - Configuration - v1.0.0

* + 1. Win - Updates - D - Microsoft Edge - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - Microsoft Edge - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:40 |
| Last modified | 10 April 2025 09:27:40 |
| Scope tags | Default |

Table 233. Basics - Win - Updates - D - Microsoft Edge - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Edge | |
| Enable component updates in Microsoft Edge | Enabled |
| Notify a user that a browser restart is recommended or required for pending updates | Enabled |
| Notify a user that a browser restart is recommended or required for pending updates (Device) | Required - Show a recurring prompt to the user indicating that a restart is required |
| Microsoft Edge Update | |
| Microsoft Edge | |
| Allow installation | Enabled |
| Allow installation | Enabled |
| Install Policy (Device) | Force Installs (Machine-Wide) |
| Prevent Desktop Shortcut creation upon install | Enabled |
| Target Channel override | Enabled |
| Target Channel (Device) | Stable |
| Update policy override | Enabled |
| Policy (Device) | Always allow updates (recommended) |
| Control updater's communication with the Experimentation and Configuration Service | Enabled |
| Control updater's communication with Experimentation and Configuration Service (Device) | Disable communication with the Experimentation and Configuration Service |
| Microsoft Edge Web View2 Runtime | |
| Allow installation | Enabled |
| Update policy override | Enabled |
| Update Policy (Device) | Always allow updates (recommended) |
| Microsoft Edge WebView | |
| Allow installation | Enabled |
| Install Policy (Device) | Force Installs (Machine-Wide) |
| Preferences | |
| Auto-update check period override | Enabled |
| Minutes between update checks (Device) | 240 |

Table 234. Settings - Win - Updates - D - Microsoft Edge - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 235. Assignments - Win - Updates - D - Microsoft Edge - v1.0.0

* + 1. Win - Updates - D - Microsoft Office - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - Microsoft Office - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:41 |
| Last modified | 10 April 2025 09:27:41 |
| Scope tags | Default |

Table 236. Basics - Win - Updates - D - Microsoft Office - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Office 2016 (Machine) | |
| Updates | |
| Don’t install extension for Microsoft Search in Bing that makes Bing the default search engine | Enabled |
| Enable Automatic Updates | Enabled |
| Hide option to enable or disable updates | Enabled |
| Online Repair | Enabled |
| Use Office CDN (if needed) (Device) | True |

Table 237. Settings - Win - Updates - D - Microsoft Office - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 238. Assignments - Win - Updates - D - Microsoft Office - v1.0.0

* + 1. Win - Updates - D - WUfB Delivery Optimisation - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - WUfB Delivery Optimisation - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:41 |
| Last modified | 10 April 2025 09:27:41 |
| Scope tags | Default |

Table 239. Basics - Win - Updates - D - WUfB Delivery Optimisation - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Delivery Optimization | |
| DO Absolute Max Cache Size | 0 |
| DO Allow VPN Peer Caching | Not allowed |
| DO Download Mode | HTTP blended with peering behind the same NAT |
| DO Group Id Source | Entra ID Tenant ID |
| DO Max Cache Age | 0 |
| DO Max Cache Size | 20 |
| DO Min Background Qos | 500 |
| DO Min Battery Percentage Allowed To Upload | 40 |
| DO Min File Size To Cache | 10 |
| DO Min RAM Allowed To Peer | 2 |
| DO Monthly Upload Data Cap | 0 |
| DO Restrict Peer Selection By | Subnet mask |

Table 240. Settings - Win - Updates - D - WUfB Delivery Optimisation - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 241. Assignments - Win - Updates - D - WUfB Delivery Optimisation - v1.0.0

* + 1. Win - Updates - D - WUfB Restart Warnings - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - D - WUfB Restart Warnings - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:42 |
| Last modified | 10 April 2025 09:27:42 |
| Scope tags | Default |

Table 242. Basics - Win - Updates - D - WUfB Restart Warnings - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Windows Update For Business | |
| Auto Restart Notification Schedule | 15 Minutes |
| Auto Restart Required Notification Dismissal | User Dismissal. |
| Schedule Imminent Restart Warning | 60 Minutes |
| Schedule Restart Warning | 8 Hours |

Table 243. Settings - Win - Updates - D - WUfB Restart Warnings - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 244. Assignments - Win - Updates - D - WUfB Restart Warnings - v1.0.0

* + 1. Win - Updates - U - Defender Updates - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Defender Updates - Broad - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Antivirus |
| Policy type | Defender Update controls |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:42 |
| Last modified | 11 April 2025 12:45:42 |
| Scope tags | Default |

Table 245. Basics - Win - Updates - U - Defender Updates - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Engine Updates Channel | Current Channel (Broad): Devices will be offered updates only after the gradual release cycle completes. Suggested to apply to a broad set of devices in your production population (~10-100%). |
| Platform Updates Channel | Current Channel (Broad): Devices will be offered updates only after the gradual release cycle completes. Suggested to apply to a broad set of devices in your production population (~10-100%). |
| Security Intelligence Updates Channel | Current Channel (Broad): Devices will be offered updates only after the gradual release cycle completes. Suggested to apply to a broad set of devices in all populations, including production. |

Table 246. Settings - Win - Updates - U - Defender Updates - Broad - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 247. Assignments - Win - Updates - U - Defender Updates - Broad - v1.0.0

* + 1. Win - Updates - U - Defender Updates - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Defender Updates - Pilot - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Antivirus |
| Policy type | Defender Update controls |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:42 |
| Last modified | 10 April 2025 09:27:42 |
| Scope tags | Default |

Table 248. Basics - Win - Updates - U - Defender Updates - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Engine Updates Channel | Current Channel (Staged): Devices will be offered updates after the monthly gradual release cycle. Suggested to apply to a small, representative part of your production population (~10%). |
| Platform Updates Channel | Current Channel (Staged): Devices will be offered updates after the monthly gradual release cycle. Suggested to apply to a small, representative part of your production population (~10%). |
| Security Intelligence Updates Channel | Current Channel (Staged): Same as Current Channel (Broad). |

Table 249. Settings - Win - Updates - U - Defender Updates - Pilot - v1.0.0

* + 1. Win - Updates - U - Defender Updates - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Defender Updates - Preview - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Antivirus |
| Policy type | Defender Update controls |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:43 |
| Last modified | 10 April 2025 09:27:43 |
| Scope tags | Default |

Table 250. Basics - Win - Updates - U - Defender Updates - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Defender | |
| Engine Updates Channel | Current Channel (Preview): Devices set to this channel will be offered updates earliest during the monthly gradual release cycle. Suggested for pre-production/validation environments. |
| Platform Updates Channel | Current Channel (Preview): Devices set to this channel will be offered updates earliest during the monthly gradual release cycle. Suggested for pre-production/validation environments. |
| Security Intelligence Updates Channel | Not configured (Default). Microsoft will either assign the device to Current Channel (Broad) or a beta channel early in the gradual release cycle. The channel selected by Microsoft might be one that receives updates early during the gradual release cycle, which may not be suitable for devices in a production or critical environment |

Table 251. Settings - Win - Updates - U - Defender Updates - Preview - v1.0.0

* + 1. Win - Updates - U - Microsoft Office - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft Office - Broad - v1.0.0 |
| Description | Cloned policy from W11 - Office - Office Configuration - V1.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:43 |
| Last modified | 17 June 2025 10:13:07 |
| Scope tags | Default |

Table 252. Basics - Win - Updates - U - Microsoft Office - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Office 2016 (Machine) | |
| Updates | |
| Delay downloading and installing updates for Office | Enabled |
| Days: (Device) | 8 |
| Update Channel | Enabled |
| Channel Name: (Device) | Monthly Enterprise Channel |
| Update Deadline | Enabled |
| Deadline: (Device) | 1 |
| Update Path | Enabled |
| Location for updates: (Device) | http://officecdn.microsoft.com/pr/55336b82-a18d-4dd6-b5f6-9e5095c314a6 |

Table 253. Settings - Win - Updates - U - Microsoft Office - Broad - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |
| Excluded Groups | | |
| Intune-Updates-Preview-Devices |  |  |

Table 254. Assignments - Win - Updates - U - Microsoft Office - Broad - v1.0.0

* + 1. Win - Updates - U - Microsoft Office - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft Office - Pilot - v1.0.0 |
| Description | Cloned policy from W11 - Office - Broad Ring - V1.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:43 |
| Last modified | 17 June 2025 10:12:50 |
| Scope tags | Default |

Table 255. Basics - Win - Updates - U - Microsoft Office - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Office 2016 (Machine) | |
| Updates | |
| Delay downloading and installing updates for Office | Enabled |
| Days: (Device) | 3 |
| Update Channel | Enabled |
| Channel Name: (Device) | Monthly Enterprise Channel |
| Update Deadline | Enabled |
| Deadline: (Device) | 1 |
| Update Path | Enabled |
| Location for updates: (Device) | http://officecdn.microsoft.com/pr/55336b82-a18d-4dd6-b5f6-9e5095c314a6 |

Table 256. Settings - Win - Updates - U - Microsoft Office - Pilot - v1.0.0

* + 1. Win - Updates - U - Microsoft Office - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft Office - Preview - v1.0.0 |
| Description | Cloned policy from W11 - Office - Broad Ring - V1.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:44 |
| Last modified | 10 April 2025 09:27:44 |
| Scope tags | Default |

Table 257. Basics - Win - Updates - U - Microsoft Office - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Microsoft Office 2016 (Machine) | |
| Updates | |
| Delay downloading and installing updates for Office | Enabled |
| Update Channel | Enabled |
| Channel Name: (Device) | Monthly Enterprise Channel |
| Update Deadline | Enabled |
| Deadline: (Device) | 1 |
| Update Path | Enabled |
| Location for updates: (Device) | http://officecdn.microsoft.com/pr/55336b82-a18d-4dd6-b5f6-9e5095c314a6 |

Table 258. Settings - Win - Updates - U - Microsoft Office - Preview - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| Intune-Updates-Preview-Devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 259. Assignments - Win - Updates - U - Microsoft Office - Preview - v1.0.0

* + 1. Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:44 |
| Last modified | 10 April 2025 09:27:44 |
| Scope tags | Default |

Table 260. Basics - Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OneDrive | |
| Set the sync app update ring | Enabled |
| Update ring: (Device) | Production |

Table 261. Settings - Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 262. Assignments - Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0

* + 1. Win - Updates - U - Microsoft OneDrive - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft OneDrive - Pilot - v1.0.0 |
| Description | Cloned policy from Win - Updates - U - Microsoft OneDrive - Broad v1.0.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:44 |
| Last modified | 10 April 2025 09:27:44 |
| Scope tags | Default |

Table 263. Basics - Win - Updates - U - Microsoft OneDrive - Pilot - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OneDrive | |
| Set the sync app update ring | Enabled |
| Update ring: (Device) | Production |

Table 264. Settings - Win - Updates - U - Microsoft OneDrive - Pilot - v1.0.0

* + 1. Win - Updates - U - Microsoft OneDrive - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Updates - U - Microsoft OneDrive - Preview - v1.0.0 |
| Description | Cloned policy from Win - Updates - U - Microsoft OneDrive - Broad - v1.0.0 |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:45 |
| Last modified | 10 April 2025 09:27:45 |
| Scope tags | Default |

Table 265. Basics - Win - Updates - U - Microsoft OneDrive - Preview - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OneDrive | |
| Set the sync app update ring | Enabled |
| Update ring: (Device) | Production |

Table 266. Settings - Win - Updates - U - Microsoft OneDrive - Preview - v1.0.0

* + 1. Win - USB Device Control - D - Device Control - v1.0.0 Device Control

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - USB Device Control - D - Device Control - v1.0.0 Device Control |
| Description | Device Control Policy the restricts access to reading and writing USB removable drives |
| Profile type | Settings catalog |
| Category | Attack surface reduction |
| Policy type | Device Control |
| Platform supported | Windows 10 and later |
| Created | 15 April 2025 11:48:17 |
| Last modified | 09 July 2025 13:28:55 |
| Scope tags | Default |

Table 267. Basics - Win - USB Device Control - D - Device Control - v1.0.0 Device Control

|  |  |
| --- | --- |
| Name | Value |
| Data Protection | |
| Allow Direct Memory Access | Block |
| Dma Guard | |
| Device Enumeration Policy | Block all (Most restrictive) |
| Type | Deny |
| Options | None |
| Access mask | Read;Write;Execute;File read;File write;File execute |
| ID | {7f884466-698b-4ac0-8407-2ac222aeca4e} |
| Name | Block All USB Storage Devices |
| ID | {3c6f11db-5843-4c67-8a43-3abfb5cd9c72} |
| Included Devices | e81ebb75-0eb2-4ed5-8336-8c2bd5a9dfc9 |
| Administrative Templates | |
| Device Installation Restrictions | |
| Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria | Enabled |
| Prevent installation of devices using drivers that match these device setup classes | Enabled |
| Also apply to matching devices that are already installed. | False |
| Prevented Classes | d48179be-ec20-11d1-b6b8-00c04fa372a7 |

Table 268. Settings - Win - USB Device Control - D - Device Control - v1.0.0 Device Control

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |
| Excluded Groups | | |
| Win-DeviceControl-ExclusionGroup |  |  |

Table 269. Assignments - Win - USB Device Control - D - Device Control - v1.0.0 Device Control

* + 1. Win - User Experience - D - Background and Lockscreen - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - User Experience - D - Background and Lockscreen - v2.0.0 |
| Description | New |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 02 July 2025 17:01:39 |
| Last modified | 02 July 2025 17:01:39 |
| Scope tags | Default |

Table 270. Basics - Win - User Experience - D - Background and Lockscreen - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Logon | |
| Always use custom logon background | Enabled |
| Show clear logon background | Enabled |
| Personalization | |
| Lock Screen Image Url | https://saitointune.blob.core.windows.net/stah/Lockscreen.jpg?sp=r&st=2025-07-02T16:00:59Z&se=2029-07-03T00:00:59Z&spr=https&sv=2024-11-04&sr=b&sig=eaeJEnQyl%2Brv%2BHA1UpkwJ%2BXTJwlTVzRu4UOuRl%2FjKQ4%3D |

Table 271. Settings - Win - User Experience - D - Background and Lockscreen - v2.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 272. Assignments - Win - User Experience - D - Background and Lockscreen - v2.0.0

* + 1. Win - User Experience - D - Feature Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - User Experience - D - Feature Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:45 |
| Last modified | 20 June 2025 09:17:49 |
| Scope tags | Default |

Table 273. Basics - Win - User Experience - D - Feature Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Administrative Templates | |
| Filesystem | |
| Enable dev drive | Disabled |
| Search | |
| Allow Cloud Search | Allowed. |
| Allow Indexing Encrypted Stores Or Items | Block |
| Disable Removable Drive Indexing | Enable. |
| Widgets | |
| Allow widgets | Not allowed. |

Table 274. Settings - Win - User Experience - D - Feature Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 275. Assignments - Win - User Experience - D - Feature Configuration - v1.0.0

* + 1. Win - User Experience - D - Storage Sense - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - User Experience - D - Storage Sense - v1.0.0 |
| Description | Added - Ellis Barrett |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 20 June 2025 16:18:12 |
| Last modified | 25 June 2025 11:16:49 |
| Scope tags | Default |

Table 276. Basics - Win - User Experience - D - Storage Sense - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Storage | |
| Allow Storage Sense Global | Allow |
| Allow Storage Sense Temporary Files Cleanup | Allow |
| Config Storage Sense Cloud Content Dehydration Threshold | 90 |
| Config Storage Sense Downloads Cleanup Threshold | 180 |
| Config Storage Sense Global Cadence | 7 |
| Config Storage Sense Recycle Bin Cleanup Threshold | 60 |

Table 277. Settings - Win - User Experience - D - Storage Sense - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 278. Assignments - Win - User Experience - D - Storage Sense - v1.0.0

* + 1. Win - User Experience - U - Start Menu - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - User Experience - U - Start Menu - v1.0.0 |
| Description | Amended - Allow pinning to taskbard.  Configures Windows 11 Taskbar and Start Menu |
| Profile type | Settings catalog |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:45 |
| Last modified | 10 July 2025 06:14:15 |
| Scope tags | Default |

Table 279. Basics - Win - User Experience - U - Start Menu - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Experience | |
| Configure Chat Icon | Disabled |
| Start | |
| Configure Start Pins | {  "pinnedList": [  { "desktopAppId": "MSEdge" },  { "desktopAppId": "Microsoft.Office.EXCEL.EXE.15" },  { "desktopAppId": "Microsoft.Office.POWERPNT.EXE.15" },  { "desktopAppId": "Microsoft.Office.OUTLOOK.EXE.15" },  { "desktopAppId": "Microsoft.Office.ONENOTE.EXE.15" },  { "desktopAppId": "Microsoft.Office.com.squirrel.Teams.Teams" },  { "packagedAppId": "Microsoft.CompanyPortal\_8wekyb3d8bbwe!App" },  { "desktopAppId": "Microsoft.Office.WINWORD.EXE.15" },  { "desktopAppId": "Microsoft.Windows.Explorer" }  ]  } |
| No Pinning To Taskbar | Disabled |
| Start Layout | <?xml version="1.0" encoding="utf-8"?> <LayoutModificationTemplate xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" xmlns:taskbar="http://schemas.microsoft.com/Start/2014/TaskbarLayout" Version="1"> <CustomTaskbarLayoutCollection PinListPlacement="Replace"> <defaultlayout:TaskbarLayout> <taskbar:TaskbarPinList> <taskbar:DesktopApp DesktopApplicationID="Microsoft.Windows.Explorer"/> <taskbar:DesktopApp DesktopApplicationID="Microsoft.Office.OUTLOOK.EXE.15"/> <taskbar:DesktopApp DesktopApplicationID="MSEdge"/> </taskbar:TaskbarPinList> </defaultlayout:TaskbarLayout> </CustomTaskbarLayoutCollection> </LayoutModificationTemplate> |

Table 280. Settings - Win - User Experience - U - Start Menu - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All users | \*StAH-Win-Filter-Baseline - All | Include |

Table 281. Assignments - Win - User Experience - U - Start Menu - v1.0.0

* + 1. Win - Windows Firewall - D - Firewall Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Windows Firewall - D - Firewall Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Firewall |
| Policy type | Windows Firewall |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:27:46 |
| Last modified | 17 June 2025 13:22:28 |
| Scope tags | Default |

Table 282. Basics - Win - Windows Firewall - D - Firewall Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Auditing | |
| Object Access Audit Filtering Platform Connection | Failure |
| Object Access Audit Filtering Platform Packet Drop | Failure |
| Firewall | |
| Disable Stateful Ftp | True |
| Enable Domain Network Firewall | True |
| Default Inbound Action for Domain Profile | Block |
| Default Outbound Action | Allow |
| Disable Inbound Notifications | True |
| Log Max File Size | 16384 |
| Disable Stealth Mode | False |
| Enable Log Dropped Packets | Enable Logging Of Dropped Packets |
| Enable Log Success Connections | Enable Logging Of Successful Connections |
| Log File Path | %SystemRoot%\System32\logfiles\firewall\domainfw.log |
| Enable Private Network Firewall | True |
| Disable Inbound Notifications | True |
| Default Outbound Action | Allow |
| Log Max File Size | 16384 |
| Default Inbound Action for Private Profile | Block |
| Enable Log Dropped Packets | Enable Logging Of Dropped Packets |
| Enable Log Success Connections | Enable Logging Of Successful Connections |
| Log File Path | %SystemRoot%\System32\logfiles\firewall\privatefw.log |
| Enable Public Network Firewall | True |
| Log Max File Size | 16384 |
| Allow Local Policy Merge | False |
| Default Outbound Action | Allow |
| Disable Inbound Notifications | True |
| Default Inbound Action for Public Profile | Block |
| Enable Log Ignored Rules | Disable Logging Of Ignored Rules |
| Enable Log Dropped Packets | Enable Logging Of Dropped Packets |
| Enable Log Success Connections | Enable Logging Of Successful Connections |
| Log File Path | %SystemRoot%\System32\logfiles\firewall\publicfw.log |
| Allow Local Ipsec Policy Merge | False |

Table 283. Settings - Win - Windows Firewall - D - Firewall Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 284. Assignments - Win - Windows Firewall - D - Firewall Configuration - v1.0.0

* + 1. Win - Windows Hello for Business - D - Disable Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Windows Hello for Business - D - Disable Configuration - v1.0.0 |
| Description |  |
| Profile type | Settings catalog |
| Category | Account protection |
| Policy type | Account Protection |
| Platform supported | Windows 10 and later |
| Created | 19 June 2025 11:23:12 |
| Last modified | 24 June 2025 11:25:06 |
| Scope tags | Default |

Table 285. Basics - Win - Windows Hello for Business - D - Disable Configuration - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Windows Hello For Business | |
| Use Windows Hello For Business (User) | false |
| Use Windows Hello For Business (Device) | false |

Table 286. Settings - Win - Windows Hello for Business - D - Disable Configuration - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 287. Assignments - Win - Windows Hello for Business - D - Disable Configuration - v1.0.0

* + 1. Win - Windows LAPS - D - LAPS Configuration - v1.0.1

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Windows LAPS - D - LAPS Configuration - v1.0.1 |
| Description | Testing new features |
| Profile type | Settings catalog |
| Category | Account protection |
| Policy type | Local admin password solution (Windows LAPS) |
| Platform supported | Windows 10 and later |
| Created | 17 April 2025 10:13:52 |
| Last modified | 17 June 2025 13:23:52 |
| Scope tags | Default |

Table 288. Basics - Win - Windows LAPS - D - LAPS Configuration - v1.0.1

|  |  |
| --- | --- |
| Name | Value |
| Backup Directory | Backup the password to Azure AD only |
| Password Age Days | 7 |
| Password Complexity | Large letters + small letters + numbers + special characters (improved readability) |
| Password Length | 21 |
| Post Authentication Actions | Reset the password and logoff the managed account: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminated. |
| Post Authentication Reset Delay | 1 |
| Automatic Account Management Enabled | The target account will be automatically managed |
| Automatic Account Management Name Or Prefix | SupportDesk |
| Automatic Account Management Randomize Name | The name of the target account will not use a random numeric suffix. |
| Automatic Account Management Target | Manage a new custom administrator account |
| Automatic Account Management Enable Account | The target account will be enabled |

Table 289. Settings - Win - Windows LAPS - D - LAPS Configuration - v1.0.1

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 290. Assignments - Win - Windows LAPS - D - LAPS Configuration - v1.0.1

* 1. Templates
     1. \*\*Win - Application Control - D - AppLocker - BLOCK - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - Application Control - D - AppLocker - BLOCK - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Custom |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 291. Basics - \*\*Win - Application Control - D - AppLocker - BLOCK - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OMA-URI Settings | |
| AppLocker AppX | |
| Name | AppLocker AppX |
| Description | Applocker Configuration for AppX |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/StoreAppsGroup/StoreApps/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Appx" EnforcementMode="Enabled">  <FilePublisherRule Id="5b2a8477-5617-4653-badd-81ee23fc2bb6" Name="All signed packaged apps" Description="Allows members of the Everyone group to run packaged apps that are signed." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="\*" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  <Exceptions>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.DesktopAppInstaller" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.Getstarted" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.MicrosoftOfficeHub" BinaryName="\*">  <BinaryVersionRange LowSection="17.4218.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Skype Software Sarl, O=Microsoft Corporation, L=Luxembourg, S=Luxembourg, C=LU" ProductName="Microsoft.SkypeApp" BinaryName="\*">  <BinaryVersionRange LowSection="3.2.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.WindowsFeedback" BinaryName="\*">  <BinaryVersionRange LowSection="10.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.WindowsStore" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePublisherRule>  </RuleCollection> |
| Applocker EXE | |
| Name | Applocker EXE |
| Description | AppLocker Configuration for EXE Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/EXEGroup/EXE/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Exe" EnforcementMode="Enabled">  <FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(Default Rule) All files" Description="Allows members of the local Administrators group to run all applications." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="cdfd5d1c-828f-4bd6-9542-1395c6088f82" Name="All files located in the Program Files folder" Description="Allows members of the Everyone group to run applications that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="38080c1b-54bc-4f7e-804d-fafb70bf781b" Name="All files located in the Windows folder" Description="Allows members of the Everyone group to run applications that are located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="CIPHER.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="FTP.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="INSTALLUTIL.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="MSBUILD.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="INTERNET EXPLORER" BinaryName="MSHTA.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET1.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NETSH.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="POWERSHELL\_ISE.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="PRESENTATIONHOST.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REG.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDT32.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDIT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGINI.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="RUNAS.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT ® WINDOWS SCRIPT HOST" BinaryName="\*SCRIPT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="WMIC.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePathRule>  <FilePublisherRule Id="27d9e82c-e5bb-4c3c-802f-bdba3c2b3dda" Name="Allow all Products and Binaries from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  <Exceptions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="CIPHER.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="FTP.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="INSTALLUTIL.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="MSBUILD.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="INTERNET EXPLORER" BinaryName="MSHTA.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET1.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NETSH.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="POWERSHELL\_ISE.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="PRESENTATIONHOST.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REG.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDT32.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDIT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGINI.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="RUNAS.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT ® WINDOWS SCRIPT HOST" BinaryName="\*SCRIPT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="WMIC.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePublisherRule>  <FilePathRule Id="b91a15a0-1086-4750-bcdd-b1aad9ab0a92" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="95b9ab17-6f3d-4f15-b93c-06cca9e1236f" Name="C:\ProgramData\Microsoft\\*" Description="Windows Defender" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="C:\ProgramData\Microsoft\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker MSI | |
| Name | AppLocker MSI |
| Description | AppLocker Configuration for MSI Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/MSIGroup/MSI/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Msi" EnforcementMode="Enabled">  <FilePathRule Id="5b290184-345a-4453-b184-45305f6d9a54" Name="(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer" Description="Allows members of the Everyone group to run all Windows Installer files located in %systemdrive%\Windows\Installer." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\Installer\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="64ad46ff-0d71-4fa0-a30b-3f3d30c5433d" Name="(Default Rule) All Windows Installer files" Description="Allows members of the local Administrators group to run all Windows Installer files." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*.\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="40ec8db8-5b89-4a9d-99e1-b5a81a783108" Name="Microsoft-signed MSI files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Information acquired from TrustedSigners.ps1" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="12d32b5e-800b-479b-8182-d063c4ce19b5" Name="%WINDIR%\IMECache\\*" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\IMECache\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker DLL | |
| Name | AppLocker DLL |
| Description | AppLocker Configuration for DLL Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/DLLGroup/DLL/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Dll" EnforcementMode="Enabled">  <FilePublisherRule Id="e4d4bc99-154b-4814-bfd5-e6fdc8b8c165" Name="All Products, from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Allows All DLLs signed by Microsoft" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="fe64f59f-6fca-45e5-a731-0f6715327c38" Name="(Default Rule) All DLLs" Description="Allows members of the local Administrators group to load all DLLs." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="860f0fa5-afd9-4929-880b-cf0c6f052c67" Name="Microsoft Windows DLLs" Description="Allows members of the Everyone group to load DLLs located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  </Exceptions>  </FilePathRule>  <FilePathRule Id="e431d080-a8e3-48d6-904b-19bda95b3fb7" Name="All DLLs located in the Program Files folder" Description="Allows members of the Everyone group to load DLLs that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="4f39bf10-f9ea-49d5-ba26-55535ba5fb35" Name="Disallow PowerShell v2 x86" Description="Explicitly deny unsigned JIT native images needed for PowerShell v2" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePathCondition Path="%WINDIR%\assembly\NativeImages\_v2.0.50727\_32\System.Management.A#\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="31d0a17e-420f-4b79-953f-d681fd69289f" Name="Disallow PowerShell v2 x64" Description="Explicitly deny unsigned JIT native images needed for PowerShell v2" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePathCondition Path="%WINDIR%\assembly\NativeImages\_v2.0.50727\_64\System.Management.A#\\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="0645a114-e55a-4d95-9511-5905489867c6" Name="Disallow PowerShell v2" Description="Explicitly deny signed DLLs needed for PowerShell v2 (implicitly allow 10.\* and above)" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT (R) WINDOWS (R) OPERATING SYSTEM" BinaryName="SYSTEM.MANAGEMENT.AUTOMATION.DLL">  <BinaryVersionRange LowSection="\*" HighSection="9.9.9.9" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="53d190c2-c82b-4f32-a1fa-ce5c2eb65861" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="1f5ba109-db69-4ee8-8a67-457e21dca38b" Name="C:\ProgramData\Microsoft\\*" Description="Windows Defender" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="C:\ProgramData\Microsoft\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker Script | |
| Name | AppLocker Script |
| Description | AppLocker Configuration for Scripts |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/ScriptGroup/Script/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Script" EnforcementMode="Enabled">  <FilePathRule Id="ed97d0cb-15ff-430f-b82c-8d7832957725" Name="(Default Rule) All scripts" Description="Allows members of the local Administrators group to run all scripts." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="742c089a-d5bc-4f1e-98dc-2535b7b164b5" Name="All scripts located in the Program Files folder" Description="Allows members of the Everyone group to run scripts that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="2d2e2715-50d1-4f32-9885-7c935e189f44" Name="All scripts located in the Windows folder" Description="Allows members of the Everyone group to run scripts that are located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%WINDIR%\registration\crmlog\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\detectionverificationdrv\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\detectionverificationdrv\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\esif\_umdf2\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\esif\_umdf2\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\helloface\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\helloface\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorscx0102\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorscx0102\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorshidclassdriver\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorshidclassdriver\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\surfacepenpairing\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\surfacepenpairing\data:\*" />  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  </Exceptions>  </FilePathRule>  <FilePathRule Id="8b003c31-cded-4a39-8ef9-f371807b5cde" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="296a8057-5f36-4e83-a24f-f7136115ffe9" Name="Microsoft-signed script files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Information acquired from TrustedSigners.ps1" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  </RuleCollection> |

Table 292. Settings - \*\*Win - Application Control - D - AppLocker - BLOCK - v1.0.0

* + 1. \*\*Win - User Experience - D - Background and Lockscreen - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | \*\*Win - User Experience - D - Background and Lockscreen - v1.0.0 |
| Description | Replaced |
| Platform supported | Windows 10 and later |
| Profile type | Device restrictions |
| Created | 10 April 2025 09:25:33 |
| Last modified | 02 July 2025 17:02:10 |
| Version | 13 |
| Scope tags | Default |

Table 293. Basics - \*\*Win - User Experience - D - Background and Lockscreen - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Locked Screen Experience | |
| Locked screen picture URL (Desktop only) | https://saitointunestah.blob.core.windows.net/lockscreen/Lockscreen.jpg?sp=r&st=2025-04-15T10:56:24Z&se=2028-08-31T18:56:24Z&spr=https&sv=2024-11-04&sr=b&sig=agaqKEGp3SBRJEhe%2BezdqTJqUZwKT3HMHqkCRrmy7FM%3D |
| Microsoft Edge Legacy (Version 45 and earlier) | |
| Start experience | |
| Allow user to change Start pages | No |
| Allow web content on new Tab page​ | Yes |
| Allow Users to change Home button | No |
| Show First Run Experience page (Mobile only) | Yes |
| Allow pop-ups | Yes |
| Send intranet traffic to Internet Explorer | No |
| Allow Microsoft compatibility list | Yes |
| Preload Start pages and new Tab page​ | Yes |
| Prelaunch Start pages and new Tab​ page | Yes |
| Favorites and search | |
| Allow changes to favorites | Yes |
| Sync favorites between Microsoft browsers (Desktop only) | No |
| Show search suggestions | Yes |
| Privacy and security | |
| Allow InPrivate browsing | Yes |
| Save browsing history | Yes |
| Clear browsing data on exit (Desktop only) | No |
| Allow Password Manager | Yes |
| Allow Autofill in forms | Yes |
| Send do-not-track headers | No |
| Show WebRTC localhost IP address | Yes |
| Allow live tile data collection | Yes |
| User can override certificate errors | Yes |
| Additional | |
| Allow Microsoft Edge browser (Mobile only) | Yes |
| Allow address bar dropdown | Yes |
| Allow full screen mode | Yes |
| Allow printing | Yes |
| Allow about flags page | Yes |
| Allow developer tools | Yes |
| Allow JavaScript | Yes |
| User can install extensions | Yes |
| Allow sideloading of developer extensions | Yes |
| Network proxy | |
| Use proxy script | Allow |

Table 294. Settings - \*\*Win - User Experience - D - Background and Lockscreen - v1.0.0

* + 1. Win - Application Control - D - AppLocker - AUDIT - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Application Control - D - AppLocker - AUDIT - v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Custom |
| Platform | Windows 10 and later |
| Scope tags | Default |

Table 295. Basics - Win - Application Control - D - AppLocker - AUDIT - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| OMA-URI Settings | |
| AppLocker AppX | |
| Name | AppLocker AppX |
| Description | AppLocker Configuration for AppX Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/StoreAppsGroup/StoreApps/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Appx" EnforcementMode="AuditOnly">  <FilePublisherRule Id="5b2a8477-5617-4653-badd-81ee23fc2bb6" Name="All signed packaged apps" Description="Allows members of the Everyone group to run packaged apps that are signed." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="\*" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  <Exceptions>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.Getstarted" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.MicrosoftOfficeHub" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Skype Software Sarl, O=Microsoft Corporation, L=Luxembourg, S=Luxembourg, C=LU" ProductName="Microsoft.SkypeApp" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.WindowsFeedback" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.WindowsStore" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.DesktopInstaller" BinaryName="\*">  <BinaryVersionRange LowSection="0.0.0.0" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePublisherRule>  </RuleCollection> |
| Applocker EXE | |
| Name | Applocker EXE |
| Description | AppLocker Configuration for EXE Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/EXEGroup/EXE/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Exe" EnforcementMode="AuditOnly">  <FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(Default Rule) All files" Description="Allows members of the local Administrators group to run all applications." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="cdfd5d1c-828f-4bd6-9542-1395c6088f82" Name="All files located in the Program Files folder" Description="Allows members of the Everyone group to run applications that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="38080c1b-54bc-4f7e-804d-fafb70bf781b" Name="All files located in the Windows folder" Description="Allows members of the Everyone group to run applications that are located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="CIPHER.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="FTP.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="INSTALLUTIL.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="MSBUILD.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="INTERNET EXPLORER" BinaryName="MSHTA.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET1.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NETSH.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="POWERSHELL\_ISE.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="PRESENTATIONHOST.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REG.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDT32.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDIT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGINI.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="RUNAS.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT ® WINDOWS SCRIPT HOST" BinaryName="\*SCRIPT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="WMIC.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePathRule>  <FilePublisherRule Id="27d9e82c-e5bb-4c3c-802f-bdba3c2b3dda" Name="Allow all Products and Binaries from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  <Exceptions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="CIPHER.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="FTP.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="INSTALLUTIL.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® .NET FRAMEWORK" BinaryName="MSBUILD.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="INTERNET EXPLORER" BinaryName="MSHTA.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NET1.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="NETSH.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="POWERSHELL\_ISE.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="PRESENTATIONHOST.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REG.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDT32.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGEDIT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="REGINI.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="RUNAS.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT ® WINDOWS SCRIPT HOST" BinaryName="\*SCRIPT.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT® WINDOWS® OPERATING SYSTEM" BinaryName="WMIC.EXE">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Exceptions>  </FilePublisherRule>  <FilePathRule Id="b91a15a0-1086-4750-bcdd-b1aad9ab0a92" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="95b9ab17-6f3d-4f15-b93c-06cca9e1236f" Name="C:\ProgramData\Microsoft\\*" Description="Windows Defender" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="C:\ProgramData\Microsoft\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker MSI | |
| Name | AppLocker MSI |
| Description | AppLocker Configuration for MSI Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/MSIGroup/MSI/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Msi" EnforcementMode="AuditOnly">  <FilePathRule Id="5b290184-345a-4453-b184-45305f6d9a54" Name="(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer" Description="Allows members of the Everyone group to run all Windows Installer files located in %systemdrive%\Windows\Installer." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\Installer\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="64ad46ff-0d71-4fa0-a30b-3f3d30c5433d" Name="(Default Rule) All Windows Installer files" Description="Allows members of the local Administrators group to run all Windows Installer files." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*.\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="40ec8db8-5b89-4a9d-99e1-b5a81a783108" Name="Microsoft-signed MSI files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Information acquired from TrustedSigners.ps1" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="12d32b5e-800b-479b-8182-d063c4ce19b5" Name="%WINDIR%\IMECache\\*" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\IMECache\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker DLL | |
| Name | AppLocker DLL |
| Description | AppLocker Configuration for DLL Files |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/DLLGroup/DLL/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Dll" EnforcementMode="AuditOnly">  <FilePublisherRule Id="e4d4bc99-154b-4814-bfd5-e6fdc8b8c165" Name="All Products, from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Allows All DLLs signed by Microsoft" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="fe64f59f-6fca-45e5-a731-0f6715327c38" Name="(Default Rule) All DLLs" Description="Allows members of the local Administrators group to load all DLLs." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="860f0fa5-afd9-4929-880b-cf0c6f052c67" Name="Microsoft Windows DLLs" Description="Allows members of the Everyone group to load DLLs located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  </Exceptions>  </FilePathRule>  <FilePathRule Id="e431d080-a8e3-48d6-904b-19bda95b3fb7" Name="All DLLs located in the Program Files folder" Description="Allows members of the Everyone group to load DLLs that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="4f39bf10-f9ea-49d5-ba26-55535ba5fb35" Name="Disallow PowerShell v2 x86" Description="Explicitly deny unsigned JIT native images needed for PowerShell v2" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePathCondition Path="%WINDIR%\assembly\NativeImages\_v2.0.50727\_32\System.Management.A#\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="31d0a17e-420f-4b79-953f-d681fd69289f" Name="Disallow PowerShell v2 x64" Description="Explicitly deny unsigned JIT native images needed for PowerShell v2" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePathCondition Path="%WINDIR%\assembly\NativeImages\_v2.0.50727\_64\System.Management.A#\\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="0645a114-e55a-4d95-9511-5905489867c6" Name="Disallow PowerShell v2" Description="Explicitly deny signed DLLs needed for PowerShell v2 (implicitly allow 10.\* and above)" UserOrGroupSid="S-1-1-0" Action="Deny">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT (R) WINDOWS (R) OPERATING SYSTEM" BinaryName="SYSTEM.MANAGEMENT.AUTOMATION.DLL">  <BinaryVersionRange LowSection="\*" HighSection="9.9.9.9" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  <FilePathRule Id="53d190c2-c82b-4f32-a1fa-ce5c2eb65861" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="1f5ba109-db69-4ee8-8a67-457e21dca38b" Name="C:\ProgramData\Microsoft\\*" Description="Windows Defender" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="C:\ProgramData\Microsoft\\*" />  </Conditions>  </FilePathRule>  </RuleCollection> |
| AppLocker Script | |
| Name | AppLocker Script |
| Description | AppLocker Configuration for Scripts |
| OMA-URI | ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/ScriptGroup/Script/Policy |
| Data type | String (XML file) |
| Value | <?xml version="1.0" encoding="utf-8"?>  <RuleCollection Type="Script" EnforcementMode="AuditOnly">  <FilePathRule Id="ed97d0cb-15ff-430f-b82c-8d7832957725" Name="(Default Rule) All scripts" Description="Allows members of the local Administrators group to run all scripts." UserOrGroupSid="S-1-5-32-544" Action="Allow">  <Conditions>  <FilePathCondition Path="\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="742c089a-d5bc-4f1e-98dc-2535b7b164b5" Name="All scripts located in the Program Files folder" Description="Allows members of the Everyone group to run scripts that are located in the Program Files folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%PROGRAMFILES%\\*" />  </Conditions>  </FilePathRule>  <FilePathRule Id="2d2e2715-50d1-4f32-9885-7c935e189f44" Name="All scripts located in the Windows folder" Description="Allows members of the Everyone group to run scripts that are located in the Windows folder." UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%WINDIR%\\*" />  </Conditions>  <Exceptions>  <FilePathCondition Path="%WINDIR%\registration\crmlog\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\detectionverificationdrv\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\detectionverificationdrv\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\esif\_umdf2\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\esif\_umdf2\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\helloface\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\helloface\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorscx0102\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorscx0102\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorshidclassdriver\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\sensorshidclassdriver\data:\*" />  <FilePathCondition Path="%WINDIR%\servicestate\surfacepenpairing\data\\*" />  <FilePathCondition Path="%WINDIR%\servicestate\surfacepenpairing\data:\*" />  <FilePathCondition Path="%SYSTEM32%\com\dmp\\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata:\*" />  <FilePathCondition Path="%SYSTEM32%\drivers\driverdata\\*" />  <FilePathCondition Path="%SYSTEM32%\fxstmp\\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys:\*" />  <FilePathCondition Path="%SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\drivers\color\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\printers\\*" />  <FilePathCondition Path="%SYSTEM32%\spool\servers\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\\*" />  <FilePathCondition Path="%SYSTEM32%\tasks\_migrated\\*" />  <FilePathCondition Path="%WINDIR%\debug\\*" />  <FilePathCondition Path="%WINDIR%\Debug\wia\\*" />  <FilePathCondition Path="%WINDIR%\pchealth\ERRORREP\\*" />  <FilePathCondition Path="%WINDIR%\registration\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\com\dmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\FxsTmp\\*" />  <FilePathCondition Path="%WINDIR%\SysWOW64\Tasks\\*" />  <FilePathCondition Path="%WINDIR%\tasks\\*" />  <FilePathCondition Path="%WINDIR%\temp\\*" />  <FilePathCondition Path="%WINDIR%\tracing:\*" />  <FilePathCondition Path="%WINDIR%\tracing\\*" />  </Exceptions>  </FilePathRule>  <FilePathRule Id="8b003c31-cded-4a39-8ef9-f371807b5cde" Name="Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" Description="Allows Everyone to execute from %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePathCondition Path="%OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\PLATFORM\\*" />  </Conditions>  </FilePathRule>  <FilePublisherRule Id="296a8057-5f36-4e83-a24f-f7136115ffe9" Name="Microsoft-signed script files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="Information acquired from TrustedSigners.ps1" UserOrGroupSid="S-1-1-0" Action="Allow">  <Conditions>  <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="\*" BinaryName="\*">  <BinaryVersionRange LowSection="\*" HighSection="\*" />  </FilePublisherCondition>  </Conditions>  </FilePublisherRule>  </RuleCollection> |

Table 296. Settings - Win - Application Control - D - AppLocker - AUDIT - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 297. Assignments - Win - Application Control - D - AppLocker - AUDIT - v1.0.0

* + 1. Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0 |
| Description |  |
| Platform supported | Windows 8.1 and later |
| Profile type | Trusted certificate |
| Created | 14 April 2025 16:16:46 |
| Last modified | 14 April 2025 16:16:46 |
| Version | 1 |
| Scope tags | Default |

Table 298. Basics - Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Trusted Certificate | |
| Certificate file | Forcepoint.cer |

Table 299. Settings - Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 300. Assignments - Win - Certificate - D - Forcepoint Trusted Cert - v1.0.0

* + 1. Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0 |
| Description |  |
| Platform supported | Windows 8.1 and later |
| Profile type | Trusted certificate |
| Created | 20 June 2025 08:20:39 |
| Last modified | 20 June 2025 08:20:39 |
| Version | 1 |
| Scope tags | Default |

Table 301. Basics - Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Trusted Certificate | |
| Certificate file | ForcepointCloudCA2044.cer |

Table 302. Settings - Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 303. Assignments - Win - Certificate - D - Forcepoint Trusted Cert - v2.0.0

* + 1. Win - Certificate - D - St Andrews Device Cert - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - D - St Andrews Device Cert - v2.0.0 |
| Description | Certificate Includes a SAN (DNS ENDS\_WITH Stah\_Entra |
| Platform supported | Windows 8.1 and later |
| Profile type | SCEP certificate |
| Created | 04 June 2025 15:30:58 |
| Last modified | 12 June 2025 17:33:47 |
| Version | 2 |
| Scope tags | Default |

Table 304. Basics - Win - Certificate - D - St Andrews Device Cert - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| SCEP Certificate | |
| Certificate type | Device |
| Subject alternative name | domainNameService;Stah\_Entra  universalResourceIdentifier;IntuneDeviceId://{{DeviceId}} |
| Certificate validity period | 1 Years |
| Key storage provider (KSP) | Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP |
| Key usage | Key encipherment;Digital signature |
| Key size (bits) | 2048 |
| Hash algorithm | SHA-2 |
| Root Certificate | |
| Root Certificate | Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0 |
| Extended key usage | Client Authentication;1.3.6.1.5.5.7.3.2 |
| Enrollment Settings | |
| Renewal threshold (%) | 20 |
| SCEP Server URLs | https://SNDESLVAP01-sahcorp.msappproxy.net/certsrv/mscep/mscep.dll |

Table 305. Settings - Win - Certificate - D - St Andrews Device Cert - v2.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 306. Assignments - Win - Certificate - D - St Andrews Device Cert - v2.0.0

* + 1. Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0 |
| Description |  |
| Platform supported | Windows 8.1 and later |
| Profile type | Trusted certificate |
| Created | 21 April 2025 10:16:44 |
| Last modified | 22 April 2025 09:37:03 |
| Version | 2 |
| Scope tags | Default |

Table 307. Basics - Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Trusted Certificate | |
| Certificate file | STAH-Issuing-CA1.cer |
| Destination store | Computer certificate store - Intermediate |

Table 308. Settings - Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 309. Assignments - Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0

* + 1. Win - Certificate - D - St Andrews Root Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - D - St Andrews Root Cert - v1.0.0 |
| Description |  |
| Platform supported | Windows 8.1 and later |
| Profile type | Trusted certificate |
| Created | 16 April 2025 15:29:32 |
| Last modified | 22 April 2025 13:48:17 |
| Version | 2 |
| Scope tags | Default |

Table 310. Basics - Win - Certificate - D - St Andrews Root Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Trusted Certificate | |
| Certificate file | STAH-Root-CA.cer |

Table 311. Settings - Win - Certificate - D - St Andrews Root Cert - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All | Include |

Table 312. Assignments - Win - Certificate - D - St Andrews Root Cert - v1.0.0

* + 1. Win - Certificate - U - St Andrews User Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Certificate - U - St Andrews User Cert - v1.0.0 |
| Description | St Andrews User Certificate |
| Platform supported | Windows 8.1 and later |
| Profile type | SCEP certificate |
| Created | 25 April 2025 15:48:30 |
| Last modified | 07 May 2025 13:20:01 |
| Version | 2 |
| Scope tags | Default |

Table 313. Basics - Win - Certificate - U - St Andrews User Cert - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| SCEP Certificate | |
| Subject alternative name | userPrincipalName;{{UserPrincipalName}} |
| Certificate validity period | 1 Years |
| Key storage provider (KSP) | Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP |
| Key usage | Key encipherment;Digital signature |
| Key size (bits) | 2048 |
| Hash algorithm | SHA-2 |
| Root Certificate | |
| Root Certificate | Win - Certificate - D - St Andrews Intermediate Cert - v1.0.0 |
| Extended key usage | Client Authentication;1.3.6.1.5.5.7.3.2 |
| Enrollment Settings | |
| Renewal threshold (%) | 20 |
| SCEP Server URLs | https://SNDESLVAP01-sahcorp.msappproxy.net/certsrv/mscep/mscep.dll/ |

Table 314. Settings - Win - Certificate - U - St Andrews User Cert - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Standard GroupTag | Include |
| Excluded Groups | | |
| W11\_Device Exclude Cert Test Group |  |  |

Table 315. Assignments - Win - Certificate - U - St Andrews User Cert - v1.0.0

* + 1. Win - Health Monitoring - D - Endpoint Analytics - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Health Monitoring - D - Endpoint Analytics - v1.0.0 |
| Description | Enable Endpoint Analytics Data collection |
| Platform supported | Windows 10 and later |
| Created | 10 April 2025 09:25:32 |
| Last modified | 10 April 2025 09:25:32 |
| Version | 1 |
| Scope tags | Default |

Table 316. Basics - Win - Health Monitoring - D - Endpoint Analytics - v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Health monitoring | |
| Health monitoring | Enable |
| Scope | Endpoint analytics |

Table 317. Settings - Win - Health Monitoring - D - Endpoint Analytics - v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | None | None |

Table 318. Assignments - Win - Health Monitoring - D - Endpoint Analytics - v1.0.0

* + 1. Win - Shared Multi User Device - D - TBA- v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Shared Multi User Device - D - TBA- v1.0.0 |
| Description |  |
| Platform supported | Windows 10 and later |
| Profile type | Shared multi-user device |
| Created | 15 April 2025 15:26:20 |
| Last modified | 15 April 2025 15:26:20 |
| Version | 1 |
| Scope tags | Default |

Table 319. Basics - Win - Shared Multi User Device - D - TBA- v1.0.0

|  |  |
| --- | --- |
| Name | Value |
| Shared multi-user device | |
| Click here for more info. | |
| Shared PC mode | Enable |
| Account management | Enabled |
| Start delete threshold(%) | 60 |
| Local Storage | Enabled |
| Power Policies | Enabled |
| Sign-in when PC wakes | Enabled |

Table 320. Settings - Win - Shared Multi User Device - D - TBA- v1.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Shared-GroupTag | Include |

Table 321. Assignments - Win - Shared Multi User Device - D - TBA- v1.0.0

* + 1. Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Basics | |
| Name | Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0 |
| Description | StAH\_Wireless\_Policy - This Policy Automates the Wifi Connection for all Users |
| Platform supported | Windows 10 and later |
| Profile type | Wi-Fi |
| Created | 11 June 2025 11:41:11 |
| Last modified | 11 June 2025 14:38:49 |
| Version | 3 |
| Scope tags | Default |

Table 322. Basics - Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0

|  |  |
| --- | --- |
| Name | Value |
| Wi-Fi | |
| Wi-Fi type | Enterprise |
| Wi-Fi name (SSID) | StAH\_Secure |
| Connection name | StAH\_Secure |
| Connect automatically when in range | Yes |
| Connect to this network, even when it is not broadcasting its SSID | Yes |
| Extensible Authentication Protocol (EAP) | |
| EAP type | EAP - TLS |
| Root certificates for server validation | |
| Root certificates for server validation | Win - Certificate - D - St Andrews Root Cert - v1.0.0 |
| Client Authentication | |
| Force Wi-Fi profile to be compliant with the Federal Information Processing Standard (FIPS) | No |

Table 323. Settings - Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0

|  |  |  |
| --- | --- | --- |
| Group | Filter | Filter mode |
| Included Groups | | |
| All devices | \*StAH-Win-Filter-Baseline - All GroupTags | Include |

Table 324. Assignments - Win - Wi-Fi Policy Profile - D - St Andrews Wi-Fi - v2.0.0