****

**TECHNICAL MANUAL**

Antivirus/Malware Software Setup

Windows 2022 AD Server

**Prepared By : Shaun Heywood  
Prepared on :** *02/07/2023*

**Table of Contents**

[Introduction 4](#_Toc139247448)

[Purpose and Scope 5](#_Toc139247449)

[Overview of Sophos 5](#_Toc139247450)

[Key Features 5](#_Toc139247451)

[Prerequisites 5](#_Toc139247452)

[Document Structure 6](#_Toc139247453)

[Document Revision History 6](#_Toc139247454)

[System Architecture 6](#_Toc139247455)

[Sophos Central/Sophos Enterprise Console: 6](#_Toc139247456)

[Endpoint Agent: 6](#_Toc139247457)

[Update Server: 7](#_Toc139247458)

[Database Server: 7](#_Toc139247459)

[Additional Components: 7](#_Toc139247460)

[Installation and Configuration 8](#_Toc139247461)

[Configuration 14](#_Toc139247462)

[User Management 18](#_Toc139247463)

[Data Ingestion 19](#_Toc139247464)

[Data Management 19](#_Toc139247465)

[Security and Access Control 20](#_Toc139247466)

[Monitoring and Troubleshooting 21](#_Toc139247467)

[Maintenance and Upgrades 22](#_Toc139247468)

[Best Practices 23](#_Toc139247469)

[Resources and References 24](#_Toc139247470)

|  |
| --- |
| Introduction |

|  |
| --- |
| Purpose and Scope The purpose of this document is to provide an introduction to Sophos Endpoint Security and Control, an industry leading Antivirus and Malware protection application.. It aims to familiarise users with the features, capabilities, and benefits of Sophos in monitoring and analysing an endpoint device for potential security threats and attacks. Overview of Sophos Developed by Sophos, a well-known provider of cybersecurity solutions, Sophos Endpoint Security and Control is a comprehensive cybersecurity solution designed to protect endpoint devices, such as desktops, laptops, and servers, from various security threats.  Sophos Endpoint Security and Control combines multiple layers of protection to safeguard endpoint devices from various threats. It offers robust malware protection, web security, device control, patch assessment to ensure a high level of security for organisations of all sizes. Key Features ● **Anti-Virus and HIPS**: Provides advanced protection against viruses and other malware while employing Host Intrusion Prevention System (HIPS) to detect and block unauthorised system modifications.  ● **Client Firewall (endpoint only):** Controls network traffic by employing a client-side firewall to monitor and block unauthorised network connections and protect against external threats.  ● **Data Control**: Safeguards sensitive data by monitoring and restricting its transfer and usage within the organisation, preventing data leaks and unauthorised access.  ● **Device Control:** Enables administrators to manage and control the usage of external devices, such as USB drives and storage devices, by enforcing policies and preventing potential security risks.  ● **Application Control**: Controls the execution of applications based on defined policies, allowing only authorised and trusted applications to run, enhancing security and preventing malware infections.  ● **Tamper Protection**: Prevents unauthorised modification or tampering of security settings and configurations, ensuring the integrity and effectiveness of endpoint protection.  ● **Exploit Prevention**: Detects and blocks exploit attempts targeting vulnerabilities in software and applications, safeguarding against targeted attacks and malware exploitation.  ● **Patch Assessment**: Scans and assesses the system for missing security patches and software updates, ensuring endpoints are up to date and protected against known vulnerabilities.  ● **Web Control**: Filters and controls web access to protect users from accessing malicious or inappropriate websites, preventing web-based threats and enforcing internet usage policies. Prerequisites You must have internet access in order to download the installation software from the Sophos Website. Operating System: Windows: Windows 7 or later, Windows Server 2008 R2 or later. Processor: Minimum dual-core processor, although a higher-end processor is recommended for better performance. RAM: Minimum 2 GB of RAM, although 4 GB or more is recommended for optimal performance. Disk Space: Minimum 4 GB of free disk space for installation. Additional space is required for storing logs, quarantine, and updates. Network: Internet connection required for software updates, licence activation, and communication with the Sophos management console (if used).  You will need the following information for installation and configuration:  ● Web address and download credentials for the Sophos Endpoint Security and Control standalone installer.  ● Address of the update source, unless you will be updating from Sophos directly.  ● Credentials that are needed to access the update source.  ● Details of the proxy server that you may be using to access the update source (the address and port number, the user credentials). Document Structure The document is organised into several sections, each focusing on specific aspects of Sophos Endpoint Security and Control. It starts with an overview of installation and initial configuration and concludes with best practices and references for further learning. Document Revision History Version 1.0 (June 2023): Initial release of the pfSense introduction document. |

|  |
| --- |
| System Architecture |
| To deliver complete endpoint security, Sophos Endpoint Security and Control uses a distributed system architecture made up of a number of software components. The function, supported deployment topologies, and hardware/resource needs of each component are described in detail below: Sophos Central/Sophos Enterprise Console:  * **Role:** These are the central management consoles for administering and configuring the Sophos Endpoint security solution. * **Functionality:** They provide a unified interface for managing policies, deploying software updates, monitoring security events, generating reports, and controlling endpoint security settings. * **Deployment Topologies:** Sophos Central is a cloud-based management platform, while Sophos Enterprise Console is an on-premises management console. * **Hardware/Resource Requirements:** The specific requirements vary based on the number of managed endpoints and the deployment topology. It is recommended to refer to the official Sophos documentation for detailed hardware and resource requirements.  Endpoint Agent:  * **Role:** The Endpoint Agent is installed on each endpoint device and serves as the client-side component that enforces security policies and communicates with the management console. * **Functionality:** It provides real-time protection against malware, enforces security policies, performs system scans, and reports security events to the management console. * **Deployment Topologies:** The Endpoint Agent is deployed on each managed endpoint device. * **Hardware/Resource Requirements:** The requirements depend on the endpoint's operating system and the specific version of Sophos Endpoint Security. The general guidelines include a minimum processor, RAM, and disk space as outlined in the previous response.  Update Server:  * **Role:** The Update Server acts as a central repository for storing and distributing security updates, software patches, and virus definition updates to the managed endpoints. * **Functionality:** It downloads updates from Sophos servers and distributes them efficiently to reduce internet bandwidth consumption and provide faster update deployment. * **Deployment Topologies:** The Update Server can be deployed in various configurations, including a standalone server or a distributed setup with multiple servers for load balancing and redundancy. * **Hardware/Resource Requirements:** The hardware requirements depend on the number of managed endpoints and the update frequency. It is recommended to allocate sufficient disk space to store update files and have enough bandwidth for efficient distribution.  Database Server:  * **Role:** The Database Server stores the configuration settings, policies, and security event logs for the Sophos Endpoint Security solution. * **Functionality:** It provides a reliable and secure repository for storing and retrieving critical data related to endpoint security management. * **Deployment Topologies:** The Database Server can be deployed as a standalone server or utilize an existing database infrastructure, such as Microsoft SQL Server or PostgreSQL. * **Hardware/Resource Requirements:** The specific requirements depend on the size of the environment and the number of managed endpoints. It is recommended to allocate sufficient disk space and ensure optimal database performance based on the expected workload.  Additional Components: Additional components, such as Sophos Central Intercept X, Sophos Mobile, or Sophos Email Gateway, can be integrated to improve the overall security posture depending on the implementation details and feature requirements.  Note: Depending on variables including the number of monitored endpoints, network environment, deployment architecture, and particular configuration choices, the hardware and resource requirements for each component may change. |

|  |
| --- |
| Installation and Configuration |
| **Locate the required download package for Sophos Endpoint Security and Control *https://www.sophos.com/en-us/support/downloads***  >> Click on SEC - Endpoint Clients    **Navigate to the following section and click >> Download**  **Supply the required details**    **The download will now begin**    **Open downloaded Installer and click the “install” button**  **The installer will now run the installation**    **And bring you to the installation wizard, click**  **Accept the EULA and click “next”**  **Click on the option – I will enter these details later, then click “next”**  **Uncheck the option – Remove third party security software, then click “next”**  **Installation is now ready to install, click “next”**  **Installation is now underway**  **Installation has now installed successfully, click “finish”** Configuration Next, click the Windows button, and then click on Sophos Endpoint Security and Control, in order to open the application    **Click on > Configure anti-virus and HIPS**    **Click on > On-access scanning**    **In the Scan for section – click the checkbox > Suspicious files Then click Apply**  **Then click OK**    **In the Other scanning options section, click all checkboxes to on**  **Then click Apply, then click OK**    **To run a scan, Navigate to File – New scan**    **Click the Administrator checkbox to select areas to be scanned**  **Next click “Save and start”** |

|  |
| --- |
| User Management |
| Sophos Endpoint Security and Control provides flexible user roles and permissions to enable granular control over user access and privileges within the management console.  Here are details about user roles and permissions, creating and managing user accounts, defining and assigning roles and capabilities, and authentication options:  **User Roles and Permissions:**   * **Admin:** Full administrative access to all features and settings of the management console, including the ability to create, modify, and delete policies, manage users, and access all reporting and monitoring functions. * **Power User:** Similar to Admin but with limited permissions, such as the ability to create and manage policies and perform certain administrative tasks but without access to critical system settings. * **Read-Only:** Allows viewing and generating reports, monitoring security events, and accessing policy settings but does not permit making any changes or modifications. * **Custom Roles:** Sophos Endpoint Security and Control also allows creating custom roles with specific permissions tailored to the organisation's needs.   **Creating and Managing User Accounts:**   * **Usernames:** User accounts are created with unique usernames that identify individual users within the management console. * **Passwords:** User accounts require secure passwords to ensure account authentication and access control. * **Email:** Email addresses can be associated with user accounts for communication purposes, such as password reset notifications or system updates.   **Defining and Assigning Roles and Capabilities:**  Within the management console, administrators can define roles and assign specific capabilities to each role.  Capabilities include permissions to perform actions such as creating or modifying policies, managing users, generating reports, and accessing specific features or settings.  Roles can be assigned to user accounts based on the required level of access and responsibilities.  **Authentication Options:**   * **Local Authentication:** Sophos Endpoint Security and Control supports local authentication, where user accounts and credentials are stored and managed within the management console itself. * **LDAP Integration:** Integration with Lightweight Directory Access Protocol (LDAP) enables authentication against an organisation's existing directory service, such as Microsoft Active Directory. * **Single Sign-On (SSO):** Sophos supports Single Sign-On authentication, allowing users to authenticate using their existing corporate credentials through SSO providers like SAML (Security Assertion Markup Language) or OAuth.   Based on the preferences of the organisation and the infrastructure already in place, these choices offer flexibility in managing user access and authentication. To ensure secure and effective management of Sophos Endpoint Security and Control, administrators can define user roles, set permissions, create and manage user accounts, and make use of numerous authentication methods. |

|  |
| --- |
| Data Ingestion |
| When looking at Sophos Endpoint Security and Control, data ingestion is the process of gathering and processing security-related data from multiple sources, such as endpoint devices and network logs. The security events that are relevant to endpoint devices are recorded by the agents that are deployed, including malware detections, file and network activity, system logs, and behaviour analysis.  Additionally, the solution can integrate with network security appliances, allowing the collection and analysis of network logs and traffic data. Logs from different sources, including endpoints, servers, network devices, and security appliances, can be aggregated and centralised for comprehensive analysis and correlation.  The collected data undergoes processing and analysis within the security solution, using sophisticated algorithms and detection techniques. This enables the detection of known malware signatures, identification of behavioural anomalies, and the detection of network-based threats. When threats are detected, real-time responses are triggered, such as quarantining infected files, blocking network connections, or initiating remediation actions.  The ingested data also serves as the basis for generating reports, visualising security trends, and providing insights into the overall security posture of the organisation. Alerts and notifications can be generated based on predefined rules or thresholds, ensuring that administrators are promptly notified of critical security events or anomalies. |

|  |
| --- |
| Data Management |
| The organisation, storage, and use of security-related data gathered by the solution are all parts of Sophos Endpoint Security and Control's, data management process. It includes a number of features like data lifecycle management, data storage, data privacy, and data retention. The length of time security data is maintained depends on organisational demands and regulatory restrictions, which administrators can establish in data retention policies.  Data related to security is kept in a centralised, secure location, either in a separate database or integrated with pre-existing database infrastructures. To guarantee effective data retrieval and analysis, sufficient storage space be allocated. By following data privacy laws and best practices, data privacy is maintained. Access controls and encryption are used to secure sensitive data and personally identifiable information (PII). Techniques for data anonymization can be employed to protect privacy while yet enabling study of aggregated trends and patterns.  The approach to data lifecycle management makes sure that data is properly handled from creation to deletion. To make the most of available storage space, cut down on expenses, and adhere to data protection laws, policies for data retention, archival, and secure erasure are established. To enable compliance with rules like GDPR, Sophos Endpoint Security and Control includes auditing and reporting features |

|  |
| --- |
| Security and Access Control |
| By implementing robust security controls, authentication mechanisms, user access management, encryption, and auditing, Sophos Endpoint Security and Control ensures the protection of the system, its data, and controlled access to its functionalities. These measures work together to mitigate risks, prevent unauthorised access, and provide a secure environment for managing and monitoring endpoint security.  Here is an explanation of key aspects of security and access control:  **Security Controls:**   * Sophos Endpoint Security and Control incorporates a range of security controls to safeguard the system from unauthorised access, data breaches, and malicious activities. * These controls include antivirus and anti-malware protection, host intrusion prevention systems (HIPS), firewall rules, data control mechanisms, and exploit prevention techniques. * These security controls work together to detect and prevent malware infections, monitor system activity, block unauthorised network connections, and protect sensitive data.   **Authentication Mechanisms:**   * + Sophos Endpoint Security and Control supports various authentication mechanisms to verify the identity of users accessing the system.   + Local Authentication: Users are authenticated against user accounts and credentials stored within the management console.   + LDAP Integration: Integration with Lightweight Directory Access Protocol (LDAP) enables authentication against an organisation's existing directory service, such as Microsoft Active Directory.   + Single Sign-On (SSO): Sophos supports Single Sign-On authentication, allowing users to authenticate using their existing corporate credentials through SSO providers like SAML or OAuth.   **User Access Management:**   * + Sophos Endpoint Security and Control provides user roles and permissions that define the level of access and privileges granted to each user.   + Administrators can assign roles and capabilities to users based on their responsibilities and access requirements.   + User roles can include admin, power user, read-only, or custom roles with specific permissions tailored to the organisation's needs.   + This user access management ensures that only authorised individuals have access to critical system settings, policy modifications, and sensitive security data.   **Encryption and Data Protection:**   * + Sophos Endpoint Security and Control employs encryption mechanisms to protect sensitive data, both in transit and at rest.   + This includes encryption of network communications, encryption of stored data, and encryption of sensitive configuration settings.   + Encryption safeguards data from unauthorised access, data breaches, and ensures the confidentiality and integrity of the information.     **Audit and Monitoring:**   * + Sophos Endpoint Security and Control includes auditing and monitoring capabilities to track and log user activities, system events, and security incidents.   + Detailed logs and audit trails provide visibility into user actions, policy changes, and security events.   + Monitoring features enable the detection of suspicious activities, potential security breaches, and the timely response to security incidents. |

|  |
| --- |
| Monitoring and Troubleshooting |
| In Sophos Endpoint Security and Control, monitoring and troubleshooting support continuous operation, performance improvement, and quick reaction to security problems. The solution enables administrators to maintain a secure and stable environment, respond to issues quickly, and protect the organisation's endpoints and network by monitoring system health, evaluating security events, detecting abnormalities, and offering troubleshooting tools.  Here is an explanation of key aspects of monitoring and troubleshooting:  **Monitoring:**   * + Sophos Endpoint Security and Control provides monitoring capabilities to track the performance and health of the system.   + Monitoring tools enable real-time visibility into the status of endpoints, network connections, and security events.   + Key metrics such as system resource utilisation, malware detections, network traffic, and policy compliance can be monitored to identify potential issues or deviations from expected behaviour.     **Event Logging and Alerting:**   * + The solution logs security events, user activities, policy changes, and system events to provide a detailed record for analysis and troubleshooting.   + Sophos Endpoint Security and Control can generate alerts and notifications based on predefined rules or thresholds, enabling administrators to promptly respond to critical security events or system failures.     **Anomaly Detection and Threat Intelligence:**   * + Sophos Endpoint Security and Control incorporates advanced analytics and threat intelligence to detect anomalies and potential security threats.   + Anomaly detection algorithms analyse system behaviour and network traffic patterns to identify deviations from normal operation, indicating possible security incidents or suspicious activities.   + Integration with threat intelligence feeds allows the solution to leverage up-to-date information on known threats and attack vectors, enhancing detection capabilities.     **Troubleshooting:**   * + In case of issues or security incidents, Sophos Endpoint Security and Control provides tools and resources for effective troubleshooting.   + The solution offers diagnostic utilities, log analysis features, and reporting capabilities to investigate and resolve issues.   + Administrators can review logs, perform forensic analysis, and generate reports to identify the root cause of problems, mitigate risks, and implement appropriate remediation actions.     **Remote Management and Support:**   * + Sophos Endpoint Security and Control supports remote management and administration, allowing administrators to troubleshoot and resolve issues from a central location.   + Remote management capabilities enable efficient support, reducing the need for physical access to endpoints or on-site troubleshooting.   + Sophos also provides technical support and resources to assist administrators in troubleshooting complex issues and implementing effective solutions. |

|  |
| --- |
| Maintenance and Upgrades |
| By performing regular maintenance tasks, applying software updates and patches, and planning version upgrades effectively, administrators can keep Sophos Endpoint Security and Control up to date, secure, and operating at optimal performance. Maintenance and upgrades are essential to address vulnerabilities, leverage new features, and ensure the ongoing protection of endpoints and network infrastructure.    Here is an explanation of key aspects of maintenance and upgrades:    **Regular Maintenance:**   * Regular maintenance tasks involve routine activities to keep the Sophos Endpoint Security and Control solution in optimal condition. * This may include tasks such as monitoring system health, checking for available software updates, reviewing security configurations, and performing system backups. * Regular maintenance helps prevent potential issues, ensures smooth operation, and minimises security risks.     **Software Updates:**   * Sophos periodically releases software updates that provide bug fixes, performance improvements, and new features. * These updates address vulnerabilities, enhance security capabilities, and improve overall system stability. * Administrators should regularly check for and apply software updates to ensure the solution is running on the latest version, benefiting from the latest security enhancements and functionality.     **Version Upgrades:**   * Version upgrades involve transitioning to a newer major release or version of Sophos Endpoint Security and Control. * Upgrades may introduce significant improvements, advanced features, and enhanced security capabilities. * Planning and executing version upgrades typically involve careful evaluation, testing, and coordination with stakeholders to minimise disruptions and ensure a smooth transition to the new version.     **Patch Management:**   * Patch management is a crucial part of maintenance and involves the timely application of security patches provided by Sophos. * These patches address known vulnerabilities and security weaknesses in the software. * Administrators should regularly assess and apply patches to safeguard the solution and protect against emerging threats. |

|  |
| --- |
| Best Practices |
| By following best practices, organisations can enhance the security posture of their IT infrastructure, optimise the performance of Sophos Endpoint Security and Control, and effectively mitigate risks. These practices help ensure the appropriate configuration, monitoring, and management of the solution, ultimately safeguarding endpoints, data, and network resources.    **Security Configuration:**   * Configure Sophos Endpoint Security and Control based on industry best practices and vendor recommendations. * Enable all necessary security features, such as antivirus protection, firewall rules, intrusion prevention, and data control mechanisms. * Regularly review and update security policies to align with evolving threats and organisational requirements.     **Regular Updates and Patching:**   * Keep the Sophos Endpoint Security and Control solution up to date by regularly applying software updates and patches. * Software updates include bug fixes, performance improvements, and new features, while patches address security vulnerabilities. * Establish a patch management process to ensure timely application of security patches to protect against emerging threats.     **System Monitoring and Logging:**   * Implement proactive monitoring and logging practices to detect and respond to security events and anomalies. * Enable event logging and configure alerting mechanisms to receive notifications of critical security events or system failures. * Regularly review logs and perform analysis to identify potential security incidents or areas for improvement.     **User Education and Awareness:**   * Educate end-users about security best practices, such as avoiding suspicious emails, not clicking on unknown links, and practising strong password hygiene. * Foster a culture of security awareness to empower users to recognize and report potential security threats or suspicious activities.     **Backup and Disaster Recovery:**   * Implement regular data backups and ensure the availability of disaster recovery plans. * Back up critical data to secure storage locations to mitigate the impact of data loss or system failure. * Test and validate the effectiveness of backup and recovery procedures to ensure data can be restored in case of an incident.     **Documentation and Change Management:**   * Maintain detailed documentation of configuration settings, procedures, and changes made to Sophos Endpoint Security and Control. * Document upgrade plans, deployment strategies, and troubleshooting procedures to ensure consistency and facilitate future maintenance and management.     **Regular Training and Certification:**   * Encourage administrators and IT staff to participate in regular training programs and obtain relevant certifications. * Stay updated with the latest security trends, technologies, and best practices to enhance the expertise and knowledge of the team responsible for managing Sophos Endpoint Security and Control. |

|  |
| --- |
| Resources and References |
| When it comes to resources and references for Sophos Endpoint Security and Control, the following sources can be helpful:    **Sophos Official Documentation:**   The official Sophos website provides comprehensive documentation, user guides, deployment guides, and product documentation for Sophos Endpoint Security and Control.  You can access these resources at the Sophos Documentation website: [*https://docs.sophos.com/*](https://docs.sophos.com/)    **Sophos Community:**  The Sophos Community is an online forum where users, administrators, and Sophos experts come together to discuss various topics related to Sophos products, including Endpoint Security and Control. You can browse through the community discussions, ask questions, and find useful information.  Access the Sophos Community at: [*https://community.sophos.com/*](https://community.sophos.com/)    **Knowledge Base Articles:**  The Sophos Knowledge Base contains a wealth of articles and technical resources covering a wide range of topics related to Sophos products. You can search for specific articles related to Sophos Endpoint Security and Control for troubleshooting, configuration guidance, and best practices.  Visit the Sophos Knowledge Base at: [*https://www.sophos.com/en-us/support/knowledgebase.aspx*](https://www.sophos.com/en-us/support/knowledgebase.aspx)    **Sophos Support:**  If you have a valid Sophos support contract, you can reach out to Sophos Support for assistance with any technical issues, troubleshooting, or specific questions related to Sophos Endpoint Security and Control. You can log in to the Sophos Support Portal or contact Sophos support directly.    **Webinars and Training:**  Sophos periodically hosts webinars and training sessions that cover various aspects of their products. These sessions can provide valuable insights into the features, capabilities, and best practices of Sophos Endpoint Security and Control. Keep an eye on the Sophos website or subscribe to their newsletters for updates on upcoming webinars and training opportunities. |