SOPHOS

# Professional Services for Central Products

Updated October 2023

# Contents

SKU - PRPCBA00ZZPCAA

# Central Endpoint/Server - Foundations

The Central Endpoint/Server - Foundations service is intended for organizations with a single location and basic requirements for Endpoint and Server protection. This service is delivered remotely for a duration of a half-day for a total of up to 4-hours. The Professional Services engineer will assist with the deployment of the Sophos Central client software and provide basic guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Endpoint/Server - Foundations engagement.

## Activities

- Activation of Sophos Central License(s)
- Endpoint/Server deployment planning
  - Competitor removal review/testing (1 product version)
  - Devise installation process
    - GPO,3rd party tools (e.g. SCCM, PDQ, etc.)
  - Review installation logs
  - Deployment testing (up to 5 devices)
- Endpoint/Server Agent GUI
  - Tamper Protection
  - Events/Logging
  - Self-Help
- Knowledge transfer and configuration of Endpoint/Server Base Policies
  - Threat Protection
    - Defining Exclusions
  - Peripheral Control
  - Web Control
- Logs and Reports
  - Events
  - Custom Reports
  - Scheduling
  - Audit Logs
- Review/Implement Active Directory Synchronization
- Communicating with Sophos Technical Support
  - Gathering Diagnose logs
- Q&A (as time permits)

SKU - PRPCDZ00ZZPCAA

# Central Endpoint/Server - Essentials

The Central Endpoint/Server - Essentials is intended for organizations with diverse operational requirements including but not limited to integration with a SIEM solution and configuring Update Cache/Message relays. This service is delivered remotely for a duration of one full day or two half-days for a total of up to 8-hours. The Professional Services engineer will assist with the deployment of the Sophos Central client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Endpoint/Server - Essentials engagement.

## Activities

- Activation of Sophos Central License(s)
- Endpoint/Server deployment planning
  - Competitor removal review/testing
    - Up to 4 products/versions
  - Devise installation process
    - GPO,3rd party tools (e.g., SCCM, PDQ, etc.)
  - Review installation logs
  - Deployment testing (up to 10 devices)
- Endpoint/Server Agent GUI
  - Tamper Protection
  - Events/Logging
  - Self-Help
- Review and configuration of up to 2 each of the following policies
  - Threat Protection
    - Defining Exclusions
  - Peripheral Control
  - Application Control
  - Web Control
  - Update Management
  - Windows Firewall
- Overview of Server Lockdown and File Integrity Monitoring concepts
- Logs and Reports
  - Events
  - Custom Reports
  - Scheduling
  - Audit Logs
- Threat Cases
  - Live Discover
- Review/Implement Active Directory Synchronization
- Installation of up to 2 Update Cache/Message Relay
- Sophos Central Alerting
  - Configuration of Email Alerting
- API Token Management for SIEM Integration
- Communicating with Sophos Technical Support
  - Gathering Diagnose logs
- Continued deployment assistance to Endpoints/Servers during the engagement
  - The number of devices deployed is wholly dependent on the customer
- Q&A (as time permits)

SKU - PRPDXA00ZZPCAA

# Central Endpoint/Server - Enterprise

The Central Endpoint/Server - Enterprise is intended for larger organizations with more complex network and operational requirements. This service is delivered remotely for a duration of two full days for a total of up to 16-hours. The Professional Services engineer will assist with the enablement of Enterprise Dashboard and the deployment of the Sophos Central client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution in an enterprise environment.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Endpoint/Server - Enterprise engagement.

## Activities

- Activation of Sophos Central License(s)
  - Activation of Enterprise Dashboard and Enablement of Master Licensing (if required)
- Enterprise Dashboard Configuration/Review
  - Enterprise Installer vs Sub-estate Installer
  - Enterprise Administration Roles
  - Global Templates Concepts
- Endpoint/Server deployment planning
  - Competitor removal review/testing (up to 5 products/versions)
  - Devise installation process
  - Review installation logs
  - Deployment testing (up to 20 devices)
  - Disk Imaging for VDI
- Review and configuration of up to 2 each of the following policies
  - Threat Protection
    - Defining Exclusions
  - Peripheral Control
  - Application Control
  - Web Control
  - Windows Firewall
- Policy Assignment - Device vs User
- Logs and Reports
  - Events
  - Custom Reports
  - Scheduling
  - Audit Logs
- Threat Cases
  - Live Discover
- Endpoint/Server Agent GUI
  - Tamper Protection
  - Events/Logging
  - Self-Help
- Review/Implement Active Directory Synchronization
- Installation of up to 2 Update Cache/Message Relay
- Sophos Central Alerting
  - Configuration of Email Alerting
  - API Token Management for SIEM Integration
- Communicating with Sophos Technical Support
- Continued deployment assistance of Endpoints/Servers during the engagement.
  - The number of devices deployed is wholly dependent on the customer.
- Q&A (as time permits)

SKU – PRPDRA00ZZPCAA

## Central Endpoint/Server + MDR Integrations

The Central Endpoint/Server + MDR Integrations service is intended for organizations with a single location and basic requirements for Endpoint and Server protection and NDR Sensor or MDR Integrations. This service is delivered remotely for a duration of up to 8 hours. A Professional Services engineer will assist with the deployment of the Sophos Central client software and provide basic guidance and knowledge transfer. In addition, an engineer will assist with the deployment of the Sophos NDR Sensor and/or MDR Integration software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Endpoint/Server + MDR Integrations engagement.

Activities

- Activation of Sophos Central License(s)
- Endpoint/Server deployment planning
    - Competitor removal review/testing (1 product version)
    - Devise installation process
        - GPO,3rd party tools (e.g. SCCM, PDQ, etc.)
    - Review installation logs
    - Deployment testing (up to 5 devices)
- Endpoint/Server Agent GUI
    - Tamper Protection
    - Events/Logging
    - Self-Help
- Knowledge transfer and configuration of Endpoint/Server Base Policies
    - Threat Protection
        - Defining Exclusions
    - Peripheral Control
    - Web Control
- Logs and Reports
    - Events
    - Custom Reports
    - Scheduling
    - Audit Logs
- Review/Implement Active Directory Synchronization
- Communicating with Sophos Technical Support
    - Gathering Diagnose logs
- Q&A (as time permits)

- Implementation of up to 2 NDR Sensors or 2 MDR Integration Packs or 1 of each
- Downloading of OVA for VMware (as needed)
- Installation of OVA Template for NDR Sensor or Log Collector (as needed)
    - Configuration of virtual host
        - CPU
        - RAM
        - HDD
        - NICs
- Best practice walk-through of Initial Setup Wizard
- Creation of LAN & WAN interfaces
- Registration of NDR Sensor
    - Synchronization with Sophos Licensing Servers
- Configuration of NDR Sensor
    - Enabling HTTPS WAN
    - Enabling Discover (TAP) Mode
    - Enabling ATP
    - Registering with Sophos Central
- Discussion on gathering network traffic
    - Creation of SPAN port
    - Attaching SPAN port to virtual NIC
- Verifying NDR Sensor data collection
    - Checking interfaces in GUI and CLI
    - Contacting Sophos NDR Team
- Walk through of Sophos Central NDR Reporting
- Q&A (as time permits)

SKU - PRPGBA00ZZPCAA

# Central Email – Essentials

This service is intended for organizations with up to 5 email domains/zones and is delivered remotely for a total of up to 8-hours.

The Professional Services engineer will assist with the configuration, knowledge transfer, guidance, and assistance with the cutover from your current solution.  This will ensure a successful cutover to Sophos Central Email enable your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Email solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Email - Essentials engagement.

## Activities

- Activation of Sophos Central License(s)
- Email Gateway deployment planning
  - Review current mail rules
    - Block/Allow lists
    - Approved URLs
    - VIP management
- Review/implement Active Directory/Azure AD synchronization
  - Or import users/distribution lists from other sources
- Configuration
  - Email Security Policies
    - SPAM
    - Banners
    - Quarantine/ User Self-Help
    - Sender checks
    - Malware Scanning
    - Time-of-click
    - VIP Management
  - Data Loss Prevention Policies
    - Attachment/Keyword handling
    - Email Encryption
    - Built-in templates
- Cutover
  - DNS changes (up to 5 domains/zones)
    - MX/SPF/DKIM records
  - O365 modifications
    - Mail flow changes for inbound and outbound mail
  - On-Premises Exchange
    - Connectors for inbound and outbound mail
  - Other mail providers compatible with Sophos Email Gateway
- Review Logs and Reporting
- Communicating with Sophos Technical Support
- Cutover Assistance
  - Verify DNS records
  - Verify mail flow and policies
  - Verify Block/Allow lists
  - Verify mail logs and quarantine items
- Scheduled post-cutover assistance
  - Next business day after cutover
- Q&A (as time permits)

## Implementation Process

- We begin with a 1-hour planning/kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation.
- The engineer will coordinate follow-up meetings during the initial call for the configuration and cutover and a post-cutover call.

*If you have more than 5 email domains/zones, additional services hours may be required to complete your implementation.*

SKU – PRPD2A00ZZPCAA

# Central Mobile - Essentials

This service is delivered remotely for a duration of 1-day or for a total of up to 8-hours

The Professional Services engineer will assist with the deployment of the Sophos Mobile client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts and advanced features in the configuration and management of the Sophos Mobile security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Mobile - Essentials engagement.

## Activities

- Activation of Sophos Central License(s)
- Device Configuration
    - Apple iOS
    - Apple OSX
    - Android
    - Chrome
    - Windows
- Policy Creation and Assignment
    - User
    - Device
    - Compliance
- Configure Mobile Email access
- Configure EAS Proxy
- Application Deployment
    - App Groups
- Mobile Threat Defense
    - 3rd party integrations (e.g. InTune, Airwatch, etc.)
- Logs and Reports
    - Events
    - Custom Reports
    - Scheduling
    - Audit Logs
- Deployment testing
    - Up to 10 devices
- Mobile Control Agent GUI
- Review/Implement Active Directory Synchronization
- Sophos Central Alerting
    - Configuration of Email Alerting
- Communicating with Sophos Technical Support
    - Gathering Diagnose logs
- Q&A (as time permits)

SKU – PRPD3A00ZZPCAA

# Central Device Encryption - Foundations

This service is delivered remotely for a duration of a half-day or for a total of up to 4-hours

The Professional Services engineer will assist with the deployment of the Sophos Central Device Encryption client software and provide guidance and knowledge transfer.  This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Device Encryption security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Device Encryption – Foundation engagement.

## Activities

- Activation of Sophos Central License(s)
- Review and configuration of up to 2 Device Encryption policies
- Policy Assignment
- Endpoint deployment planning
    - Review process for migration from current product
    - Review Bitlocker requirements on Endpoints
    - Review Group Policy Objects for Bitlocker
    - Devise installation process
        - Review setup of software deployment via GPO or 3rd party tools
        - Provide installation script
    - Review installation logs
    - Deployment testing
        - Up to 5 devices
- Endpoint Recovery Procedures
    - Retrieve Recovery Key
    - Change Bitlocker Authentication Passcode
- Endpoint Agent GUI
    - Tamper Protection
    - Events/Logging
    - Self-Help
- Logs and Reports
    - Events
    - Custom Reports
    - Scheduling
    - Audit Logs
- Communicating with Sophos Technical Support
    - Gathering Diagnose logs
- Q&A (as time permits)

SKU PRPH4E00ZZPCAA

## Central Endpoint/Server Health Check

The purpose of the Central Endpoint Health Check is to assess the current Sophos Central Endpoint/Server policies and provide recommendations to help improve your organizations security posture using Sophos Central.

The goal is to understand, document, and advise on your current configuration. It is not intended to perform troubleshooting or impact any immediate changes to the environment or resolve open issues. After the engagement, the engineer will compile the results and provide documentation within 2 business days.

The engineer will review and provide guidance on the following:

- Global Settings
    - General
        - Role Management
        - API Credentials
        - Tamper Protection
        - Website Management
        - Global Exclusions
        - Allowed Applications
        - Manage Update Caches and Message Relays
        - HTTPS Updating
        - Configure email alerts
    - Endpoint Protection
        - Controlled Updates
        - SSL/TLS decryption of HTTPS websites
        - Data Lake uploads (XDR only)
    - Server Protection
        - Controlled Updates
        - Data Lake uploads (XDR only)
- Endpoint Policies (up to 2 of each policy type)
    - Endpoint Threat Protection
        - Exclusions
    - Peripheral Control
    - Web Control
    - Update Management
- Server Policies (up to 2 of each policy type)
    - Server Threat Protection
        - Exclusions
    - Peripheral Control
    - Web Control
    - Update Management
    - File Integrity Monitoring

SKU - PCAZ3C00ZZPCAA

## Security Posture Assessment

The goal is to understand and advise on your current security posture and is not intended to perform troubleshooting or impact any immediate changes to the environment or resolve open issues. The Security Posture Assessment begins with a conference call and remote screen sharing session which may last up to 4-hours. The following will be performed during the meeting and documentation will be provided within 2 business days.

### Sophos Central Health Check

Our Health Check of your Central environment is designed to make sure you are following our best practices, ensuring you get the most out of our endpoint solution.

The engineer will review and provide guidance on the following:

- Global Settings
  - General
    - Tamper Protection
    - Global Exclusions
    - HTTPS Updating
    - Multi-factor Authentication (MFA)
  - Endpoint Protection
    - Controlled Updates
  - Server Protection
    - Manage Update Caches and Message Relays
    - Controlled Updates
- Endpoint Policies (up to 2 of each policy type)
  - Endpoint Threat Protection
  - Peripheral Control
  - Web Control
- Server Policies (up to 2 of each policy type)
  - Server Threat Protection
  - Peripheral Control
  - Web Control
  - File Integrity Monitoring

### NIST Assessment

The NIST Cyber Security Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. Completing the assessment will provide you a report giving insight into your organization’s current maturity. You will have actionable recommendations to improve your security posture.

### EASM and Dark Web Scanning

The final task we will perform is an external device discovery scan, locating systems that are available on the public internet. We will complete vulnerability scans on these devices to assess if they are susceptible to attack. Last but not least, we will look to see if any of your corporate information can be found on the Dark Web.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS