Sophos Central Enterprise
Help
Contents

About this Help.........................................................................................................................................1
About Sophos Central Enterprise............................................................................................................ 2
Dashboard................................................................................................................................................ 3
Alerts......................................................................................................................................................... 4
Logs.......................................................................................................................................................... 5
Audit Logs...................................................................................................................................... 5
Sub-estates............................................................................................................................................... 7
Unlink sub-estates......................................................................................................................... 9
Delete sub-estates....................................................................................................................... 10
Licenses.................................................................................................................................................. 11
Trials....................................................................................................................................................... 12
Settings and Policies.............................................................................................................................. 13
  Configure email alerts................................................................................................................. 13
  Administrators.......................................................................................................................... 14
Set up multi-factor authentication.............................................................................................. 20
Sign in using an authenticator.................................................................................................... 21
Federated sign-in.......................................................................................................................... 21
Global templates.......................................................................................................................... 23
Deployment............................................................................................................................................. 59
  Installer command-line options for Windows.............................................................................. 59
  Installer command-line options for Mac...................................................................................... 64
Explore Products.................................................................................................................................... 67
Global Security News............................................................................................................................. 68
Account Details...................................................................................................................................... 69
  Account Preferences.................................................................................................................. 69
  Licensing...................................................................................................................................... 70
Enterprise Master Licenses.............................................................................................................. 72
Supported Web Browsers...................................................................................................................... 74
Get additional help................................................................................................................................. 75
Legal notices.......................................................................................................................................... 76

(2020/09/08)
1 About this Help

This Help tells you how to use all the features in Sophos Central Enterprise.
If you can't find the help you need here, go to the Support section of our website and search there.
This finds knowledge base articles or discussions in the Sophos Community.

**Tip**
Sign in to Sophos Central Enterprise [here](#) and we'll help you get started.

You can sign in with your Microsoft sign-in details if your administrator has set this up. Click **Sign in with Microsoft** and enter your Microsoft sign-in details.
2 About Sophos Central Enterprise

Sophos Central Enterprise enables distributed security management. It lets administrators manage the security of an organization divided into multiple sub-estates. For example an organization that has several sites can manage the security for each site as a separate sub-estate.

Enterprise administrators can manage the sub-estates using Sophos Central Enterprise. Sophos Central Enterprise includes several predefined administration roles that divide security administration by responsibility level. Each enterprise administrator has the SuperAdmin role for each of the sub-estates.

Each sub-estate has its own Sophos Central Admin account with its own administrators. You can:

- View and manage your enterprise sub-estates and their licenses.
- View and manage your enterprise administrators.

**Related concepts**

Administrators (page 14)

You can view and manage the Sophos Central Enterprise administrators.
3 Dashboard

The Dashboard provides access to the most important information about your sub-estates at a quick glance.

It consists of these areas:

Alerts

Alerts indicates the number of High, Medium and Info Alerts associated with your sub-estates. These are aggregated alerts across all of your managed sub-estates. Click on a number to view more information. For example, clicking on the “High Alerts” number will take you to the Alerts page with the “Show High Alerts Only” filter applied.

Click View All Alerts to see all the alerts associated with your sub-estates.

License Management

It shows license information that requires, or will soon require an action (for example, the number of licenses that are expired or near expiration, over the limit license usage, the number of trials).

When you click on a category, you are taken to a more detailed view of the licensing information in that category. For example, clicking on “Near Expiration” will take you to the Sub-Estates Licenses page with the “Near Expiration” filter applied. There, you can see the date when the license expires, name of the sub-estate, name, ID and type of the license, as well as usage limit and actual usage.
4 Alerts

You can view and manage the alerts for your Sophos Central Admin sub-estates that have enterprise management enabled.

To search for alerts associated with a sub-estate, enter the sub-estate's name or the beginning of the sub-estate's name. To display all the records again, clear the search field.

You can filter the list of alerts based on their priority. You can choose to:

- Show All Alerts (default)
- Show High Alerts Only
- Show Medium Alerts Only
- Show Info Alerts Only

Launch Sophos Central

If enterprise management is enabled in the sub-estate's Sophos Central Admin account, you can open their Sophos Central Admin console and take action on alerts.

If the sub-estate hasn't enabled enterprise management you can't see this option.

Select the alert and click Launch Sophos Central Admin.

Note
Enterprise management can only be enabled by the sub-estate's Sophos Central Admin administrator. The administrator must have the SuperAdmin role to do this.

To enable enterprise management the sub-estate's Sophos Central Admin administrator should turn it on in Sophos Central Admin in the Account Details > Account Preferences option.

Export to CSV

You can export the list of alerts to a comma separated value (CSV) file, which you can then view, for example in Microsoft Excel.
5 Logs

The Logs pages provide reports on the security features in Sophos Central Enterprise and your sub-estates.

You can view and export a record of all activities that are monitored by Sophos Central Enterprise using the Audit Log report.

Related concepts
Audit Logs (page 5)
You can export reports of actions carried out in Sophos Central Enterprise and actions by sub-estates managed from Sophos Central Enterprise.

5.1 Audit Logs

You can export reports of actions carried out in Sophos Central Enterprise and actions by sub-estates managed from Sophos Central Enterprise.

Note
Your admin role affects what you see in the Audit log. If you don't have access to a sub-estate, you don't see that sub-estate's actions.

To find the Audit Log reports, go to the Logs page.

All activities for the past 7 days are shown in the Audit Log by default. You can view all activities for up to 90 days. You can export an Audit Log report containing a record of all activities in the last 90 days.

• **Date**: Date and time when the activity or change occurred.
• **Event Location**: Where the event occurred. This could be Sophos Central Enterprise or one of the sub-estates.
• **Modified by**: The Sophos Central Enterprise account that made the change or signed in.
• **Item type**: The type of activity or change. For example *Users* and *Groups* were changed.
• **Item modified**: What was added, changed or deleted. For example the name of a new user that was added.
• **Description**: More details about the activity or change. For example a successful authentication by a Sophos Central Admin account.
• **IP address**: The IP address from where the activity or change was carried out.

Filter

You can filter the Audit Log by date range, event locations and by search results. You must click Update to apply the filters.

• **Date**: Use this option to set the date range for the activities you want to view. You can select any date within the last 90 days. The date range works with the Search field and the Audit Log shows
the items related to your selected date range and search term. If you do not enter a search term or filter, the Audit Log shows all activities for your selected date range.

- **Event locations**: You can filter results by All event locations, Enterprise only or Sub-estates only.

**Search**

There is a limited search available. The Audit Log shows the items related to your search term and the selected date range. If you do not set a date range the Audit Log shows the items related to your search term for the last 7 days, by default. You can search by:

- **Sub-estate**: Shows all changes and activity made from a specific sub-estate over the selected date range.
- **IP address**: Shows all changes and activity from an IP address over the selected date range.
- **Modified by**: Shows all changes and actions made by a Sophos Central Enterprise Admin account over the selected date range.

**Export**

You can export an Audit Log report that contains a record of activities for a selected date range or the last 90 days. You can filter the Audit Log before exporting. Search filtering applies to all export options. The date range does not.

To export an audit report:

1. Filter the Audit Log, if required. Select **Update** to apply the filters to the Audit Log.
2. Click **Export** on the right-hand side of the Audit Log page and choose an option from the drop-down list.
   - **CSV of current view** or **PDF of current view**: Exports the current view as a comma separated file or as a PDF file. If you select one of these options all currently selected filters are applied to the exported file.
   - **CSV of past 90 days** or **PDF of past 90 days**: Exports activities from the past 90 days as a comma separated file or as a PDF file. If you select one of these options only search filtering is applied to the exported file.
3. Review the audit report to check that it contains the information you require.
4. Change the audit report name.

Audit reports are exported as audit.csv or audit.pdf.
6 Sub-estates

When you turn on Enterprise Management from a Sophos Central Admin account, any other accounts associated with your customer account are linked to your Sophos Central Enterprise account as sub-estates.

To allow access the sub-estate's Sophos Central Admin administrator must:

1. In Sophos Central Admin, click **Account Details > Account Preferences**.
   This shows that Enterprise Management has been turned on for the organization and also shows the enterprise administrator's details.

2. Switch on enterprise admin access to the Sophos Central Admin account.

The **Sub-Estates** page lists your sub-estates and provides an at-a-glance view of the number of licenses they are using in each of the available categories and the status of those licenses.

You can also:

- Create new sub-estates.
- Unlink sub-estates.
- Delete sub-estates.
- Check which sub-estates have allowed the enterprise admins to access and manage their Sophos Central Admin account.

**Restriction**

The sub-estate's Sophos Central Admin administrator has to allow the enterprise admins to access their account. The administrator must have the SuperAdmin role to do this. Only an Enterprise Super Admin can turn off the opt-in once it is enabled.

Search

To search for a sub-estate, enter the sub-estate's name or the beginning of the sub-estate's name.

To display all the records again, clear the search field.

New Sub-Estate

You can create new sub-estates that allow enterprise admin access automatically.

To create a new sub-estate:

1. Click **New Sub-Estate**.
2. Enter the administrator details for the new sub-estate.
3. Select a **Data storage region**. Choose from **Germany, Ireland, and United States**.
   The default region for a sub-estate is the region of the primary sub-estate. The primary sub-estate is the Sophos Central Admin account where Enterprise Management was originally turned on.
4. Read and accept the privacy policy and license agreement.
5. Click **Create Sub-Estate**.
   The new sub-estate is shown in the list. The administrator is sent an email with setup instructions.

6. Purchase a license for the sub-estate. Once you have done this, you can manage the sub-estate in Sophos Central Enterprise.

**Start Sophos Central Admin**

If the sub-estate has allowed enterprise admin access, you can open the sub-estate's Sophos Central Admin account.

If the sub-estate hasn't allowed access, you can't see this option.

Select the sub-estate and click **Launch Sophos Central Admin**.

**License Details**

You can view the license information associated with a sub-estate. To do this, select the sub-estate and click **License Details**.

**License information**

The licenses used by each sub-estate are listed under the license name. Click a license name to review information about the product associated with the license.

**Sub-estate name**

To change a sub-estate's name, do one of the following:

- 1. Click the sub-estate's name to show **Contact Info**.
- 2. Click **Edit**.
- 3. Change the name and click **Save**.
- 1. Select the sub-estate and click **License Details**.
- 2. Click **Edit**.
3. Change the name and click **Save**.

Data storage location

To find out where a sub-estate's data is stored, do one of the following:

- Click the sub-estate's name to show **Contact Info**.
- Select the sub-estate and click **License Details**.

The location is shown next to **Data storage location**.

**Related tasks**

**Unlink sub-estates** (page 9)
You can unlink a sub-estate if you want to disassociate it from an enterprise and operate the sub-estate as an independent Sophos Central Admin account with its own licenses.

**Delete sub-estates** (page 10)
Deleting a sub-estate removes the sub-estate from your enterprise and marks it for permanent deletion (after 90 days).

6.1 Unlink sub-estates

You can unlink a sub-estate if you want to disassociate it from an enterprise and operate the sub-estate as an independent Sophos Central Admin account with its own licenses.

**Restriction**
You can only unlink sub-estates if you are a Super Admin.

If you unlink a sub-estate from an enterprise that is using master licensing the resulting unlinked Sophos Central Admin account will only have trial licenses. You need to add a new license key after the 30 day trial period.

There are restrictions on unlinking sub-estates:

- You can't unlink the primary sub-estate that was used to enable enterprise management.
- All sub-estates that you are unlinking must have an active administrator with the Super Admin role.
**Sophos Central Enterprise**

- You can't unlink sub-estates that are in the process of converting to master licensing. You can unlink sub-estates after conversion is complete.

1. Select the sub-estates you want to unlink.
2. Click **More** and then click **Unlink sub-estate from this enterprise**.
3. Review the list of selected sub-estates.
4. Select **Yes, unlink the sub-estate(s) from this enterprise**.
5. Click **Unlink**.

Unlinked sub-estates are still part of the enterprise but you can't manage them in Sophos Central Enterprise.

**Opt-in to Sophos Central Enterprise** is turned off for these sub-estate accounts in Sophos Central Admin.

**Note:**
- You can't re-enable enterprise management in Sophos Central Admin for an unlinked sub-estate.
- You can't opt in to enterprise management for an unlinked sub-estate.

If you want to re-link a sub-estate or establish a new enterprise using the unlinked sub-estate you need to contact Sophos Support to request the sub-estate is linked to a different Sophos Central Enterprise account.

### 6.2 Delete sub-estates

Deleting a sub-estate removes the sub-estate from your enterprise and marks it for permanent deletion (after 90 days).

**Restriction**

You can only delete sub-estates if you are a Super Admin.

When you delete a sub-estate all the associated admins are also deleted. This releases the email addresses associated with the administration accounts. You can then use these email addresses with other accounts.

**Note**

You can't access the deleted sub-estate once it is marked for deletion.

There are restrictions on deleting sub-estates:
- You can't delete the primary sub-estate that was used to enable Sophos Central Enterprise.
- You can't delete sub-estates with full licenses.
1. Select the sub-estates you want to delete.
   - You can delete sub-estates with trial and expired licenses.
2. Click **More** and then click **Delete sub-estate**.
3. Review the list of selected sub-estates.
4. Select **Yes, permanently delete the sub-estate(s)**.
5. Click **Delete**.
7 Licenses

You can view your sub-estates’ licenses using the **Sub-Estate Licenses** page.

It contains the list of Sophos Central licenses associated with your sub-estates. It shows the name of the sub-estate, the license, its start and end date, and the usage.

It also shows the total number of licenses as well as the number of licenses that are near expiration, expired, or over their usage limit, and the number of trial licenses.

You can click on the number of each license type to filter the list of licenses. For example, clicking on the "Expired" number shows the expired licenses.

Search

To search for a sub-estate, enter the sub-estate’s name or the beginning of the sub-estate’s name. To display all the records again, clear the search field.

Export to CSV

You can export the license list to a comma separated value (CSV) file, which you can then view, for example in Microsoft Excel.

*Note*

This option is only available in the "All licenses" view.
8 Trials

The **Trials** page contains the list of trial Sophos Central licenses that your sub-estates have. It shows the trial license, its ID and which sub-estate is using it. You can see the start date and expiry date for the license and its usage.

The active trial licenses from the last 30 days are shown by default. You can show the active trial licenses for the last 60 or 90 days or all licenses.
9 Settings and Policies

You can manage administrators, sign-in settings, alerts, access to the provisioning API, and global templates.

You can manage settings and base policies in global templates.

9.1 Configure email alerts

You can manage how you and your sub-estates receive email alerts.

You can only do this for Sophos Central Admin accounts you manage. You can't manage email alerts for accounts that your sub-estates manage themselves.

Click Enterprise control if you want to manage email alerts.

You can turn Enterprise control off again if you want your sub-estates to manage their own email alerts. Click Enterprise control to do this. This also restores any settings previously specified by sub-estates.

You can:

• Manage which administrators get email alerts.
• Add distribution lists or email address that you want to receive email alerts.
• Manage the frequency of email alerts.
• Set custom rules to specify which alerts an administrator gets.
• Edit the exceptions that have been set up for individual alert types in your sub-estates accounts.

Restriction
You must be an Enterprise Super Admin to manage email alerts.

Administrators

The Administrators list shows who receives email alerts by default.

The list shows the name, email address and admin role for each administrator.

You can choose which administrators you want to receive alerts. Select Yes or No in the administrator's details to do this.

Distribution lists

You can manage the distribution lists or email addresses that you want to receive email alerts.

Use this option to add the email addresses of your distribution lists, ticketing system or people you want to notify about alerts, but do not have access to Sophos Central Enterprise.

If you want to provide access to Sophos Central Enterprise, add the person as an administrator.

• Select Add email address. Enter the email address and give a description and select Save.
• To remove an email address, select the address and select Delete.
**Frequency**

You can manage the frequency with which admins receive email alerts. You can set the frequency depending on one of the following:

- The severity of the alert.
- The product.
- The category the alert is in.

You can only use one of these attributes to set frequency.

You can choose between **Immediately**, **Hourly**, **Daily** or **Never**. Your choices are used for alerts from all your sub-estates.

**Note**

The **Hourly** and **Daily** options aren't a digest of all alerts generated in the specified time. Admins will get an email for each alert.

**Custom rules**

By default, admins get all email alerts for all your sub-estates.

Custom rules make it easy to specify that some admins will only get alerts for certain sub-estates, products, or events.

To see details of a rule, click the fold-out arrow next to it in the list.

To pause a rule, edit it or delete it, select the appropriate icon beside it in the list. Hover over icons to see what they do.

**Exceptions**

The **Exceptions** list shows the exceptions you have set. These change the frequency of email alerts for certain alert types.

You set them in individual alert details on the **Alerts** page in Sophos Central Admin. You can also edit them here.

**9.2 Administrators**

You can view and manage the Sophos Central Enterprise administrators.

On the **Administrators** page, you can assign roles to administrators. Administration roles divide security administration by responsibility level. Sophos Central Enterprise includes several predefined roles.

Each administrator has the Super Admin role for each of the sub-estate's Sophos Central accounts.

You can add custom roles and assign them to administrators to manage security administration by responsibility level and product.

You can search the list of enterprise administrators, add, manage and delete administrators.
You can reset the multi-factor authentication for an administrator. You can also change roles for administrators.

To search for an administrator, enter the name, email address, or sub-estate (or just enter the beginning of your search term). To display all the administrators again, clear the search field.

To view the details for an administrator click on the administrator’s name.

Related concepts
Roles (page 15)
You can assign roles to administrators if you are an Sophos Central Enterprise Super Admin.

Related tasks
Add administrators (page 17)
You can add administrators if you are an Enterprise Super Admin.

Edit administrators (page 17)
You can edit the details for an administrator if you are an Enterprise Super Admin.

Add a custom role (page 18)
You can add custom roles if you are an Enterprise Super Admin.

Change roles (page 19)
You can change the assigned roles for administrators if you are an Enterprise Super Admin.

Delete custom role (page 20)
You can delete custom roles if you’re an Enterprise Super Admin.

Delete administrators (page 20)
You can delete administrators if you are an Enterprise Super Admin.

Set up multi-factor authentication (page 20)
You can manage your multi-factor authentication sign-in settings.

9.2.1 Roles

You can assign roles to administrators if you are an Sophos Central Enterprise Super Admin.

Administration roles divide security administration by responsibility level. Sophos Central Enterprise includes several predefined roles. These roles cannot be edited or deleted. This is the access level for an administrator.

The options are Enterprise Super Admin, Enterprise Admin, Enterprise Help Desk or Enterprise Read-only.

An Enterprise Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

Enterprise Super Admin

There must be at least one administrator with an Enterprise Super Admin role.

This role has access to everything in Sophos Central Enterprise and Sophos Central Admin.

In addition administrators can:

• Add and remove other enterprise admins.
• Choose the sub-estates that the other admins are allowed to access.
• Create, edit, assign and delete custom roles.
Sophos Central Enterprise

- Enable master licensing.
- Start trials after master licensing is enabled.
- Create a sub-estate.
- Reset the multi-factor authentication/PIN.
- Unlink sub-estates.
- Delete sub-estates.
- Disable enterprise control over an individual licensed enterprise.

Enterprise Admin

This role has access to everything in Sophos Central Enterprise and Sophos Central Admin. In addition administrators can only access their designated sub-estates.

Enterprise Help Desk

This role has access to everything in Sophos Central Enterprise and Sophos Central Admin. In addition administrators can:
- Only access their designated sub-estates.
- Look at sensitive logs or reports.
- Receive and clear alerts.
- Update the Sophos agent software on a computer.
- Scan computers.
- Modify the co-branding for their sub-estates in Sophos Central Admin.

Enterprise Read-only

This role has access to everything in Sophos Central Enterprise and Sophos Central Admin. In addition administrators can:
- Only access their designated sub-estates.
- Look at sensitive logs or reports.
- Receive alerts.

Related tasks

Add administrators (page 17)
You can add administrators if you are an Enterprise Super Admin.

Edit administrators (page 17)
You can edit the details for an administrator if you are an Enterprise Super Admin.

Add a custom role (page 18)
You can add custom roles if you are an Enterprise Super Admin.

Change roles (page 19)
You can change the assigned roles for administrators if you are an Enterprise Super Admin.

Delete custom role (page 20)
You can delete custom roles if you’re an Enterprise Super Admin.

Delete administrators (page 20)
You can delete administrators if you are an Enterprise Super Admin.

9.2.2 Add administrators

You can add administrators if you are an Enterprise Super Admin.

To add an administrator:
1. On the Manage Administrators page select Admins.
2. Select Add an Enterprise Admin.
3. Enter the new administrator’s name and email address.
4. Select a role.
5. Select the sub-estates they can access. You must choose at least one sub-estate.
   You can give the administrator the ability to select some sub-estates or all sub-estates. If you allow them access to all sub-estates this includes all existing and future sub-estates. If you add a new Enterprise Super Admin they have access to all sub-estates.
6. Select Save.

The administrator is sent an email with setup instructions.

Related tasks
Edit administrators (page 17)
You can edit the details for an administrator if you are an Enterprise Super Admin.

Delete administrators (page 20)
You can delete administrators if you are an Enterprise Super Admin.

9.2.3 Edit administrators

You can edit the details for an administrator if you are an Enterprise Super Admin.

To edit the details for an administrator:
1. Select the administrator’s name in Manage Administrators.
2. Select Edit.
3. Edit the details for the administrator, for example change their email address, role or sub-estate access.
   You can give the administrator the ability to select some sub-estates or all sub-estates. If you allow them access to all sub-estates this includes all existing and future sub-estates.
4. Select Save.

Related tasks
Add administrators (page 17)
You can add administrators if you are an Enterprise Super Admin.

Delete administrators (page 20)
You can delete administrators if you are an Enterprise Super Admin.

9.2.4 Add a custom role

You can add custom roles if you are an Enterprise Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

**Restriction**

If a role doesn’t have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.

The shared settings are:

- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
- Blocked item
- Bandwidth usage (Encryption access required)
- HTTPS updating
- DLP rules
- Manage content control list
- Reject network connections
- EDR threat analysis center

To create a custom role:

1. On the Manage Administrators page, select Roles and Add role.
2. Give the custom role a name and a description.
3. Select the Base role you want to use as the basis for the custom role. For example, if you choose Help Desk as the Base role, administrators with the custom role have Help Desk permissions in Sophos Central Enterprise.
4. Choose the product and access type you want the role to have in Sophos Central Admin. For example, you create a custom role called Endpoint Help Desk. This custom role uses Read-only as its Base role and Endpoint Protection as its selected product with an access type of Help Desk.

This custom role allows any administrators assigned to this role to access Endpoint Protection in Sophos Central Admin with Help Desk permissions. They have the same permissions in Sophos Central Enterprise as an administrator with the Enterprise Read-only role.

a) Choose more than one product, if required.
   
   You can choose different access types for different products.
   
   For example you can create a custom role that has Help Desk access permissions for Endpoint Protection and Read-only access for Mobile. You can set the permissions for all other products to None. This means that the custom role only has access in Sophos Central
Admin to **Endpoint Protection** with **Help Desk** permissions and **Mobile** with **Read-only** permissions.

5. Choose the additional access and management options for the custom role in Sophos Central Admin.
   
   - **Enable access to logs & reports.**
   - **Enable policy management (add, edit, and delete).**
   - **Enable policy assignment to users, device, etc.** (turn policies on and off; and add users, user groups, devices, and device groups to existing policies).

   For example, this allows an Enterprise Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

   **Note**
   
   These additional options only apply to the selected products for the custom role.

   The additional options are the same for all products and access types for the custom role.

6. Select **Save**.

   You can now assign this role to administrators.

**Related concepts**

**Roles** (page 15)

You can assign roles to administrators if you are an Sophos Central Enterprise Super Admin.

**Related tasks**

**Change roles** (page 19)

You can change the assigned roles for administrators if you are an **Enterprise Super Admin**.

**Delete custom role** (page 20)

You can delete custom roles if you're an Enterprise Super Admin.

---

### 9.2.5 Change roles

You can change the assigned roles for administrators if you are an **Enterprise Super Admin**.

You can change roles for multiple administrators at the same time.

**Restriction**

You can't change roles for administrators who are currently signed in.

To change roles:

1. Select an administrator’s name in **Manage Administrators**. This opens the admin details page.
   
   Select an administrator with the role you want to assign to other administrators. For example select a read-only administrator if you want to assign administrators to that role.

2. Select the role. This opens the role type page.

3. Select **Edit** above the **Role Members** list.

4. Add administrators from the **Available admins** list and select **Save**.

**Related concepts**

**Roles** (page 15)
You can assign roles to administrators if you are an Sophos Central Enterprise Super Admin.

**Related tasks**
- Add a custom role (page 18)
  You can add custom roles if you are an Enterprise Super Admin.
- Delete custom role (page 20)
  You can delete custom roles if you’re an Enterprise Super Admin.

### 9.2.6 Delete custom role

You can delete custom roles if you’re an Enterprise Super Admin.

You can only delete custom roles. You can't delete roles that have administrators assigned to them. You must change their role first.

1. On the Manage Administrators page select Roles.
2. Select the roles you want to remove and select Delete.
3. Select Delete to confirm role deletion.

**Related concepts**
- Roles (page 15)
  You can assign roles to administrators if you are an Sophos Central Enterprise Super Admin.

**Related tasks**
- Change roles (page 19)
  You can change the assigned roles for administrators if you are an Enterprise Super Admin.
- Add a custom role (page 18)
  You can add custom roles if you are an Enterprise Super Admin.
- Delete administrators (page 20)
  You can delete administrators if you are an Enterprise Super Admin.

### 9.2.7 Delete administrators

You can delete administrators if you are an Enterprise Super Admin.

An Enterprise Super Admin can't delete themselves.

To delete an administrator:

- In Manage Administrators:
  a) Select Admins.
  b) Select the administrator you want to delete and select Delete.
- Alternatively click on an administrator’s name in Manage Administrators and select Delete admin on the Admin Details page.

### 9.3 Set up multi-factor authentication

You can manage your multi-factor authentication sign-in settings.

If you have reset multi-factor authentication for an enterprise administrator they need to set it up again. Here’s what to do to set up MFA:
1. At the sign-in screen, enter your user ID (email address) and password.

2. In the next dialog:
   a) Enter the security code that has been sent to you in an email.
   b) Create a 6-digit PIN. This enables you to use email as an authentication method.

3. In the next dialog, choose authentication type.

4. In Verify Your Device scan the QR code and enter the security code. The code is either displayed in the Sophos/Google Authenticator app or an SMS text.

Sophos Central Enterprise opens.

You can sign in with email authentication if you don't have access to Sophos/Google Authenticator or SMS text. To do this enter the verification code sent to you by email and your 6-digit PIN.

9.4 Sign in using an authenticator

Find out how to sign in to Sophos Central Enterprise using the Sophos or Google authenticator.

The account you use must already be enrolled in multi-factor authentication. To verify this, see Set up multi-factor authentication.

To sign in, do as follows:

1. Sign in to Sophos Central Enterprise.
   The Verify Your Login pop-up appears.

   ![Verify Your Login pop-up]

2. Enter the code from the authenticator and click Submit.

   You are now signed in.

9.5 Federated sign-in

You must be an Enterprise Super Admin to turn on federated sign-in for your administrators.

You can allow your administrators to sign in to Sophos Central Enterprise using their Sophos Central Enterprise sign-in credentials, their Microsoft sign-in credentials, or both.

If you turn on federated sign-in for Sophos Central Enterprise it doesn't apply to your sub-estates.

Restriction
An Enterprise admin can't use the same Microsoft sign-in credentials to sign in to Sophos Central Admin.
Note
Sophos Central Enterprise is not supported on mobile devices.

You can also add custom sign-in rules for specific administrators.

Using Microsoft credentials to sign in

Before an administrator can sign in using their Microsoft credentials, the following must happen:

• An Azure AD administrator must grant consent (permission) to use the credentials stored in your organization's Azure AD tenant to sign in to Sophos Central.
  This consent applies to Sophos Central Admin, Sophos Central Enterprise and the Self-Service Portal.
  Once an Azure AD administrator gives consent, it means your Azure AD tenant trusts Sophos Central and your administrators can sign in with their Microsoft credentials.

• You need to turn on federated sign-in. You need to choose which credentials your administrators use to sign in.

If you want to allow your administrators to use their Microsoft credentials only to sign in, you also need to know the following:

• What happens if you change to using Sophos Central Enterprise sign-in credentials only?
  Administrators won't have a password set up to validate against. They need to use "Reset Password" to set a new password and then sign in.

• Can administrators reset their passwords if you turn on Sign in with Microsoft credentials only?
  No, they won't receive reset password emails.

Note
Your administrators can sign in using their Microsoft credentials if the email address associated with their Sophos Central Enterprise credentials matches their Microsoft sign-in credentials.

Related tasks
Turn on federated sign-in (page 22)
Follow these instructions to turn on federated sign-in and choose how your administrators sign in.

Related information
Understanding Azure AD application consent experiences
knowledge base article 133433
knowledge base article 133587

9.5.1 Turn on federated sign-in

Follow these instructions to turn on federated sign-in and choose how your administrators sign in.

If you want your administrators to sign in using their Microsoft credentials, you must:

• Make sure you have an Azure Active Directory (AD) account with Microsoft. Azure AD is Microsoft’s cloud-based identity and access management service.
• Get consent and authorization from your Azure AD admin to use your company’s Azure AD with Sophos Central Enterprise.
• Make sure you have a Sophos Central Enterprise account that matches your Azure AD account (the emails must match).
• You must be a Enterprise Super Admin to turn on federated sign-in.

To choose how your administrators sign in:

1. Click Federated Sign-in in Settings.
2. Make sure that an Azure AD admin has given consent for federated sign-in, if you want to allow administrators to sign in using their Microsoft credentials.

Note
If an Azure AD admin doesn’t give permission for Sophos Central Enterprise to use federated sign-in before you turn on Sign in with Microsoft credentials only, federated sign-in will fail.

3. Choose how you want your administrators to sign in.
   If you choose Sign in with Microsoft credentials only you can send an email to newly-added administrators to tell them how to sign in.
4. Add custom sign-in rules for specific administrators, if required.
   a) If you want your administrators to sign in using their Microsoft credentials only, we recommend that you create a by-pass custom rule for one of the administrators. Click Add Admins to do this.
   b) Allow them to sign in using either their Sophos Central Enterprise or Microsoft credentials.
5. Click Save.

Related concepts
Federated sign-in (page 21)
You must be an Enterprise Super Admin to turn on federated sign-in for your administrators.

9.6 Global templates

You can create templates that consist of settings and base policies. You can apply these templates to groups of your sub-estates.

Restriction
Admins with the Enterprise Super Admin role can manage global templates.

A global template lets you:
• Apply the same settings to all sub-estates in a group.
• Stop sub-estates from changing your settings.
• Update templates and push changes to sub-estates.

The Global Templates page shows your templates, the number of sub-estates they apply to, when the template was last pushed and their push status.

You can filter the templates by searching for sub-estates.

Click a template name to see the sub-estates, global settings and base policies associated with it.
To push a template to sub-estates, select the template and click **Push**. Pushing a template can take a few minutes.

**Related concepts**
- **Template** (page 24)
  You can see the sub-estates, base polices and global settings associated with the template.

**Related tasks**
- **Create a template** (page 24)
  You can create a global template.
- **Clone a template** (page 25)
  You can clone an existing template, assign it to new sub-estates, and edit the settings and policies. You can then push the new template to your sub-estates.

### 9.6.1 Create a template

You can create a global template.

**Restriction**
- Admins with the Enterprise Super Admin role can create templates.

To create a template:

1. Go to **Settings & Policies** and click **Global Templates**.
2. Click **Global templates**.
3. Give the template a name. You can also give it a description.
4. Click **Edit sub-estates**.
5. Click the sub-estates you want to apply this global template to and add them to the **Assigned sub-estates** list.
   - **Available managed sub-estates** are sub-estates that are not assigned to any other template.
6. Click **Save**.
7. Click **Global Settings** and click on the settings you want to change.
8. Select and click on the base policies you want to change.
9. Click **Push to sub-estates** and then click **Push** to confirm.
   - You need to push the template to your sub-estates. Changes take effect after you have pushed the template.

All assigned sub-estates have their base policies and global settings locked in Sophos Central Admin.

### 9.6.2 Template

You can see the sub-estates, base polices and global settings associated with the template.

**Restriction**
- Admins with the Enterprise Super Admin role can manage templates.

You can edit, clone or delete templates and push them to sub-estates.
The **Sub-estates** tab lists the sub-estates associated with the template.

Use the **Global Settings** tab to specify security settings that apply to your sub-estates.

Use the **Base policies** tab to customize base policies for your sub-estates.

**Related concepts**

*Base Policies* (page 31)

Each feature has a base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

**Related tasks**

*Create a template* (page 24)

You can create a global template.

*Clone a template* (page 25)

You can clone an existing template, assign it to new sub-estates, and edit the settings and policies. You can then push the new template to your sub-estates.

*Edit a template* (page 26)

You can edit an existing template, assign it to new sub-estates, or edit the settings and policies. You can then push the new template to your sub-estates.

*Delete a template* (page 27)

Deleting a template leaves sub-estates with the last base policies and settings pushed to them.

*Push a template* (page 26)

When you add a sub-estates to a template, all the global and policy settings covered by the template are locked in Sophos Central Admin. They take effect when you push the template.

**Clone a template**

You can clone an existing template, assign it to new sub-estates, and edit the settings and policies. You can then push the new template to your sub-estates.

The list of assigned sub-estates is not cloned.

**Restriction**

Admins with the Enterprise Super Admin role can clone templates.

To clone a template:

1. Select the template.
2. Select **Clone**.
3. Give the template a new name. You can also give it a description.
4. Select **Edit sub-estates**.
5. Select the sub-estates you want to apply this global template to and add them to the **Assigned sub-estates** list.
6. **Available managed sub-estates** are sub-estates that are not assigned to any other template.
7. Edit the **Global Settings**.
8. Select **Edit sub-estates**.
9. Edit the **Base policies**.
10. Push the template to your sub-estates.

Changes take effect after you have pushed the template.
**Related tasks**

*Push a template* (page 26)
When you add a sub-estates to a template, all the global and policy settings covered by the template are locked in Sophos Central Admin. They take effect when you push the template.

**Edit a template**

You can edit an existing template, assign it to new sub-estates, or edit the settings and policies. You can then push the new template to your sub-estates.

**Restriction**

Admins with the Enterprise Super Admin role can edit templates.

1. Select the template.
2. Select *Edit*.
3. Select *Edit sub-estates*, if required. You can:
   - Select sub-estates you want to apply this global template to and add them to the *Assigned sub-estates* list. Click *Ok* to confirm the additions.
     Assigning a sub-estate to a template locks the base policy in Sophos Central Admin.
   - Remove sub-estates from a template by selecting them in the *Assigned sub-estates* list and adding them to the *Available managed sub-estates* list. Click *Unassign* to confirm their removal.
     Removing a sub-estate leaves them with the last settings pushed to them. Sub-estates can reset the base policies and settings in Sophos Central Admin.
4. Edit the *Global Settings*.
5. Edit the *Base policies*.
6. Push the template to your sub-estates.
   Changes take effect after you have pushed the template.

**Related tasks**

*Push a template* (page 26)
When you add a sub-estates to a template, all the global and policy settings covered by the template are locked in Sophos Central Admin. They take effect when you push the template.

**Push a template**

When you add a sub-estates to a template, all the global and policy settings covered by the template are locked in Sophos Central Admin. They take effect when you push the template.

Pushing a template can take a few minutes.

**Restriction**

Admins with the Enterprise Super Admin role can push templates.

To push a template:
1. Select the template.
2. Select *Push to sub-estates*.
3. Select *Push* to confirm.
The status of push is indicated on the Global Templates page. It also shows the last time the template was pushed and who pushed it.

Delete a template

Deleting a template leaves sub-estates with the last base policies and settings pushed to them.

**Restriction**
Admins with the Enterprise Super Admin role can delete templates.

To delete a template:
1. Select the template.
2. Select **Delete**.
3. Confirm that you want to delete the files by selecting **Yes, I want to delete this template** and clicking **Delete**.

Sub-estates can reset the base policies and settings in Sophos Central Admin.

9.6.3 Sub-estates

When you add a sub-estate to a template, all the base policies and settings covered by the template are locked. They take effect when you push the template.

**Restriction**
Admins with the Enterprise Super Admin role can manage global templates.

Sub-estates you add won’t be able to change any base policies or custom global settings shown in the template.

To change the list of sub-estates:
1. Select **Edit sub-estates**.
2. Select sub-estates in the **Available managed sub-estates** list and add them to the **Assigned sub-estates** list.
   
   Available managed sub-estates are sub-estates not assigned to any other template.
3. You can remove sub-estates by selecting them in the **Assigned sub-estates** list and adding them to the **Available managed sub-estates** list.
4. Select **Save**.
5. Select **Push to sub-estates**. Pushing a template can take a few minutes.

9.6.4 Global Settings

Use **Global Settings** to specify security settings that apply to your sub-estates.

The **Global Settings** tab is used to specify security settings that apply to your sub-estates. Sub-estates won’t be able to change these custom settings. You can specify different security settings depending on the global template you apply to your sub-estate.

The pages displayed depend on the features included in your licenses.
Some settings are only available in the base policies.

**Related concepts**

**Base Policies** (page 31)
Each feature has a base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

**Allowed applications** (page 28)
Our software may sometimes detect an application as a threat when you know it is safe.

**Related tasks**

**Website Management** (page 30)
You can extend the website filtering provided by Sophos Central.

**Global exclusions** (page 29)
You can exclude files, websites and applications from scanning for threats, as described below.

**Allowed applications**

Our software may sometimes detect an application as a threat when you know it is safe.

If you have allowed applications in Sophos Central Admin you can't see them in the list of allowed applications in Sophos Central Enterprise.

Any applications that you allow in Sophos Central Enterprise are merged into the list of allowed applications in Sophos Central Admin when you push a template to your sub-estates.

**About allowed applications**

Our software detects threats that are previously unknown. However, it may sometimes identify an application as a threat, even though you know that it’s safe. When this happens, you can “allow” the application. This does as follows:

- Prevents this detection from happening again.
- Restores all copies that have been cleaned up (removed from computers).

Alternatively, you can allow an application in advance, so that it won't be detected when you install it for users. Think carefully before you do this as it reduces your protection.

**Allow an application in advance**

You can allow an application in advance, so that it won't be detected when you install it for users.

Only allow an application if you know it's safe but think it might be detected as a threat. Think carefully as doing this reduces your protection.

Note that:

- You can only allow the application by using its path (location).
- This allows the application to start, but we'll still check the application for threats, exploits and malicious behavior when it's running.

1. On the **Global Settings** page, click **Allowed Applications**.
2. Select **Add apps by path**.
3. Enter a path. You can use variables if the application is in a different location on different computers.
Edit the path for an allowed application

You can change the path that you specified when you allowed an application.

1. On the **Allowed Applications** page, find the application. The current path is shown in the details.
2. Click the edit icon (the pen) on the far right of the page.
3. In the **Edit path** dialog, enter the new path.

When you edit a path, details of the original detection (user, computer and path) are removed from the list.

Start detecting an application again

If you want Sophos to start detecting and removing an application again, you remove it from the **Allowed Applications** list.

Select the application and click **Remove** (in the upper right of the page).

**Related information**

**Sophos Threat Center**

Global exclusions

You can exclude files, websites and applications from scanning for threats, as described below.

We'll still check the excluded items for exploits.

**Note**

These exclusions will apply to all your users (and their devices) and servers. If you want them to apply only to certain users or servers, use the exclusions in the Sophos Central Admin policies instead.

Enterprise administrators can push global exclusions from Sophos Central Enterprise. These are added to the **Global exclusions** list in Sophos Central Admin.

Sub-estate administrators:

- Won't be able to add exclusions directly to the list in Sophos Central Admin.
- Will still be able to add exclusions from the events list. These are not added to the **Global exclusions** list in Sophos Central Enterprise.

1. In **Global Settings**, click **Global exclusions**.
2. Click **Add Exclusion** (on the right of the page).
   The **Add Exclusion** dialog is displayed.
3. In the **Exclusion Type** drop-down list, select a type of item to exclude (file or folder, website or potentially unwanted application).
4. Specify the item or items you want to exclude. The following rules apply:
   - **File or folder (Mac/Linux)**. You can exclude a folder or file. You can use the wildcards ? and *.
     Examples: /Volumes/excluded (Mac)/mnt/hgfs/excluded (Linux)
• **File or folder (Sophos Security VM).** On Windows guest VMs protected by a Sophos security VM, you can exclude a drive, folder or file by full path. You can use the wildcards * and ? but only for file names.

• **Process (Windows).** You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application, not just the process name shown in Task Manager. Example: `%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe`. You can use wildcards and variables.

**Note**
To see all processes or other items that you need to exclude for an application, see the application vendor’s documentation.

• **Website.** Websites can be specified as IP address, IP address range (in CIDR notation), or domain. Examples:
  — IP address: 192.168.0.1
  — IP address range: 192.168.0.0/24
  — The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range. Thus /24 equals the netmask 11111111.11111111.11111111.00000000. In our example, the range includes all IP addresses starting with 192.168.0.
  — Domain: google.com

• **Potentially Unwanted Application.** Here, you can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system.

5. For File or folder exclusions, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.
6. Click **Add** or **Add Another.** The exclusion is added to the exclusions list.

**Website Management**

You can extend the website filtering provided by Sophos Central.

In **Website Management**, you can use a website list to tag websites. This puts them in groups, which are like custom categories. You can then use them in Web Control policies in Sophos Central Admin to control these websites for certain users.

If you think Sophos has put a website in the wrong category, you can ask us to change it.

1. Click **Add** in the upper right of the page.
   The **Add Website Customization** dialog is displayed.
2. Enter sites.
   Entries in the website list can be single URLs, full domains, top-level domains (TLDs), IP addresses, or CIDR ranges.

**Note**
Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.
3. Select a **Category Override** if you want to use a different category to the one that Sophos has applied to the sites you have entered. This changes the category for all your users.

   For example, you have a Web Control policy that allows the **Shopping** category but blocks the **News** category. If you add www.amazon.com to the website list and select **News** as the category override, www.amazon.com is blocked for all your users. However, other shopping websites are still allowed.

4. **Under Add Tags**, type one or more tag names to associate tags with the sites you have entered.

   Tags can be used when creating web control policies in Sophos Central Admin.

5. **Enter text in the Comments text box.**

   It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.

6. **Click Save.**

   Your entry will be added to the website list.

### 9.6.5 Base Policies

Each feature has a base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

**Restriction**

Admins with the Enterprise Super Admin role can manage base policies.

If you're new to policies, read this page to find out how base policies work.

**What is a policy?**

A policy is a set of options that Sophos Central applies to protected users, devices or servers.

There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

Users, devices and servers have separate policies.

**What is a global base policy?**

For some features, like threat protection, Sophos configures the base policy with the best practice settings. You can leave it unchanged if you want to.

For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.

The base policy is always available and is used if you don't have other policies activated.

**Note**

You can't disable or delete the base policy.
What is in each global base policy?

A global base policy lets you:

- Configure base policy settings for your sub-estates.
- Specify which sub-estates the policy applies to. You do this using a Global Template.

**Restriction**
Sub-estate administrators won’t be able to change any of the base policies shown here.

Which base policies can I set globally?

You can set up a base policy for Email Security.
You can set up a base policy for Device Encryption.
You can set up base policies for Endpoint Protection.
You can set up base policies for Server Protection.

**Related concepts**
*Edit a base policy* (page 33)
You can edit and assign base policies to users, groups or devices.

*Endpoint: Peripheral Control* (page 34)
Peripheral control lets you control access to peripherals and removable media.

*Endpoint: Threat Protection* (page 35)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

*Endpoint: Update Management* (page 39)
The Update Management base policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

*Endpoint: Web Control* (page 39)
You need to configure the Web Control options to protect users and computers. There are no default options.

*Endpoint: Windows Firewall* (page 41)
You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your computers using a Windows Firewall base policy.

*Server: Lockdown* (page 42)
Server Lockdown prevents unauthorized software from running on servers.

*Server: Peripheral Control* (page 43)
Peripheral control lets you control access to peripherals and removable media.

*Server: Threat Protection* (page 45)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

*Server: Update Management* (page 50)
The Update Management base policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

*Server: Web Control* (page 50)
Web Control lets you restrict access to certain categories of website.

**Server: Windows Firewall** (page 51)
You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your servers using a Windows Firewall base policy.

**Encryption: Device Encryption** (page 52)
Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault on Macs. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

**Email Security** (page 54)
Use this policy to apply security settings to email.

**Template** (page 24)
You can see the sub-estates, base polices and global settings associated with the template.

**Related tasks**

**Endpoint: Application Control** (page 33)
Application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.

**Server: Application Control** (page 41)
Application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.

**Edit a base policy**

You can edit and assign base policies to users, groups or devices.

**Restriction**
Admins with the Enterprise Super Admin role can edit base policies.

1. Click on a template on the **Global Templates** page.
2. Go to **Base policies**.
   
   You see a list of base policies.
3. Find the base policy you want to edit and click it.
4. In the base policy, use the tabs to:
   - Assign the base policy. For example, assign it to specific users, groups or devices.
   - Enter settings for the base policy. See the Help topic for that base policy type.
   - Enable or disable the base policy.

**Endpoint: Application Control**

Application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.

We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. In the **Controlled Applications** list, click **Add/Edit List**.
   
   This opens a dialog where you can see the categories of applications that you can control. Sophos supplies and updates the list.
2. Select an application category, for example **Browser plug-in**.
   
   A full list of the applications in that category is displayed in the right-hand table.
3. We recommend that you select **Select all applications**. You'll refine your selection later.
4. Click **Save to List** and repeat for each category you want to control.
   If you want to control an application that isn't in the list supplied by Sophos, you can ask to have it added. Click the "Application Control Request" link at the bottom of Application Control settings.

5. In **Detection Options**:
   - Click **Detect controlled applications when users access them (You will be notified).**
   - Click **Block the detected application.**
     If you chose to control any new applications added by Sophos, those new applications will now be blocked.

6. In **Desktop Messaging** you can add a message to the standard notification. If you leave the message box empty only the standard message is shown.
   **Desktop Messaging** is on by default. If you switch off **Desktop Messaging** you will not see any notification messages related to Application Control.
   a) Enter the text you want to add.

**Endpoint: Peripheral Control**
Peripheral control lets you control access to peripherals and removable media.
If you need to exempt individual peripherals from that control you should use a Peripheral Control Policy in Sophos Central Admin.

**Manage Peripherals**
In **Manage Peripherals**, select how you want to control peripherals:

- **Monitor but do not block (all peripherals will be allowed)**: If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you can't set access rules for them.

- **Control access by peripheral type and add exemptions**: If you select this, you can go on to set access policies for peripheral types.

**Restriction**
You can't add peripheral exemptions at the global level, so you will need to do this at the sub-estate level.

**Set Access Policies**
The **MTP/PTP** category includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.
For each peripheral type, you can change the access policy:

- **Allow**: Peripherals are not restricted in any way.
- **Block**: Peripherals are not allowed at all.
- **Read Only**: Peripherals can be accessed only for reading.
The Bluetooth, Infrared, and Modem categories don't have the **Read Only** option.
The Wireless Network Adaptor category has a **Block Bridged** option. This prevents bridging of two networks.

**Desktop Messaging**

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Desktop Messaging** is on by default.

**Note**

If you switch off **Desktop Messaging** you will not see any notification messages related to peripheral control.

Click in the message box and enter the text you want to add.

**Endpoint: Threat Protection**

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

SophosLabs can independently control which files are scanned. They may add or remove scanning of certain file types in order to provide the best protection.

**Use recommended settings**

Click **Use recommended settings** if you want to use the settings Sophos recommends. These provide the best protection you can have without complex configuration.

If we change our recommendations in future, we’ll automatically update your policy with new settings.

The recommended settings offer:

- Detection of known malware.
- In-the-cloud checks to enable detection of the latest malware known to Sophos.
- Proactive detection of malware that has not been seen before.
- Automatic cleanup of malware.

**Deep Learning**

Deep learning uses advanced machine learning to detect threats. It can identify known and previously unknown malware and potentially unwanted applications without using signatures.

Deep learning is only available with Sophos Intercept X.

**Live Protection**

Live Protection checks suspicious files against the latest malware in the SophosLabs database.

You can select these options:
**Use Live Protection to check the latest threat information from SophosLabs online:** This checks files during real-time scanning.

**Real-time Scanning - Local Files and Network Shares**

Real-time scanning scans files as users attempt to access them, and allows access if the file is clean.

Local files are scanned by default. You can also select **Remote files** to scan files on network shares.

**Real-time Scanning - Internet**

Real-time scanning scans internet resources as users attempt to access them. You can select these options:

- **Scan downloads in progress**
- **Block access to malicious websites:** This denies access to websites that are known to host malware.
- **Detect low-reputation files:** This warns if a download has a low reputation. The reputation is based on a file's source, how often it is downloaded and other factors.

You can specify:

- **Action to take on low-reputation downloads:** If you select **Prompt user**, users will see a warning when they download a low-reputation file. They can then trust or delete the file. This is the default setting.
- **Reputation level:** If you select **Strict**, medium-reputation as well as low-reputation files will be detected. The default setting is **Recommended**.

**Remediation**

Remediation options are:

- **Automatically clean up malware:** Sophos Central will try to clean up detected malware automatically.
  
  If the cleanup succeeds, the malware detected alert is deleted from the alerts list. The detection and cleanup are shown in the events list.

  Automatic cleanup doesn't apply to PE (Portable Executable) files, like applications, libraries and system files. PE files are quarantined and can be restored.

- **Enable Threat Case creation:** Threat cases let you investigate the chain of events in a malware attack and identify areas where you can improve your security.

- **Allow computers to send data on suspicious files, network events, and admin tool activity to Sophos Central:** This sends details of potential threats to Sophos. Ensure it's turned on in any policy for computers where you want to do threat searches.

**Note**

This option is available if you have Intercept X Advanced with EDR.
**Restriction**

You must turn this option on in both Endpoint and Server Protection to use Intercept X Advanced with EDR.

---

**Runtime Protection**

Runtime protection protects against threats by detecting suspicious or malicious behavior or traffic. You can select:

- **Protect document files from ransomware (CryptoGuard):** This protects document files against malware that restricts access to files, and then demands a fee to release them. You can also choose to protect 64-bit computers against ransomware run from a remote location.

- **Protect from master boot record ransomware:** This protects the computer from ransomware that encrypts the master boot record (and so prevents startup) and from attacks that wipe the hard disk.

- **Protect critical functions in web browsers (Safe Browsing):** This protects your web browsers against exploitation by malware.

- **Mitigate exploits in vulnerable applications:** This protects the applications most prone to exploitation by malware. You can select which application types to protect.

- **Protect processes:** This helps prevent the hijacking of legitimate applications by malware. You can select these options:
  - **Prevent process hollowing attacks:** This prevents process replacement attacks.
  - **Prevent DLLs loading from untrusted folders:** This prevents loading of .DLL files from untrusted folders.
  - **Prevent credential theft:** This prevents the theft of passwords and hash information from memory, registry, or hard disk.
  - **Prevent code cave utilisation:** This detects malicious code that's been inserted into another, legitimate application.
  - **Prevent APC violation:** This prevents attacks from using Application Procedure Calls (APC) to run their code.
  - **Prevent privilege escalation:** This prevents attacks from escalating a low-privilege process to higher privileges to access your systems.

- ** Protect network traffic:** You can select these options:
  - ** Detect malicious connections to command and control servers:** This detects traffic between an endpoint computer and a server that indicates a possible attempt to take control of the endpoint computer.
  - **Prevent malicious network traffic with packet inspection (IPS):** This scans traffic at the lowest level and blocks threats before they can harm the operating system or applications.

- **Detect malicious behavior (HIPS):** This protects against threats that are not yet known. It does this by detecting and blocking behavior that is known to be malicious or is suspicious.

- **AMSI Protection (with enhanced scan for script-based threats):** This protects against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). Code forwarded via AMSI is scanned before it runs and the applications used to run the code are notified of threats by Sophos. If a threat is detected, an event is logged.
Advanced Settings

These settings are for testing or troubleshooting only. We recommend that you leave them set to the defaults.

Device Isolation

If you select this option, devices will isolate themselves from your network if their health is red. A device's health is red if it has threats detected, has out-of-date software, isn't compliant with policy, or isn't properly protected.

You can still manage isolated devices from Sophos Central. You can also use scanning exclusions or global exclusions to give limited access to them for troubleshooting.

You can't remove these devices from isolation. They will communicate with the network again once their health is green.

Scheduled Scanning

Scheduled scanning performs a scan at a time or times that you specify.

You can select these options:

- **Enable scheduled scan**: This lets you define a time and one or more days when scanning should be performed.

  **Note**
  The scheduled scan time is the time on the endpoint computers (not a UTC time).

- **Enable deep scanning**: If you select this option, archives are scanned during scheduled scans. This may increase the system load and make scanning significantly slower.

Exclusions

You can exclude files, folders, websites or applications from scanning for threats, as described below.

We'll still check excluded items for exploits. However, you can stop checking for an exploit that has already been detected (use a Detected Exploits exclusion).

Exclusions set in a policy are only used for the users the policy applies to.

**Note**
If you want to apply exclusions to all your users and servers, set up global exclusions on the **Global Settings > Global Exclusions** page.

To create a policy scanning exclusion:

1. Click **Add Exclusion** (on the right of the page).
   - The **Add Exclusion** dialog is displayed.
2. In the **Exclusion Type** drop-down list, select a type of item to exclude (file or folder, website, potentially unwanted application, or device isolation).

3. Specify the item or items you want to exclude.

4. For **File or folder** exclusions only, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

5. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings, and click **Update**.

**Desktop Messaging**

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Enable Desktop Messaging for Threat Protection** is on by default. If you switch it off you will not see any notification messages related to threat protection.

Enter the text you want to add.

**Related information**

knowledge base article 121461

**Endpoint: Update Management**

The Update Management base policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

**Restriction**

You can’t set this policy for users.

Enable **Scheduled Updates** and select the day and time when you want product updates to become available.

Remember that if computers aren’t on, they won’t get the update until the next time they start.

**Endpoint: Web Control**

You need to configure the Web Control options to protect users and computers. There are no default options.

There are no default options.

**Additional security options**

Click **Additional security options** to configure access to advertisements, uncategorized sites and risky downloads.

**Block risky downloads**: This option blocks risky file types, but allows advertisements and uncategorized files.

**None**: This option allows risky file types, advertisements and uncategorized files.

**Let me specify**: This allows you to set advertisements and uncategorized file types to **Allow**, **Block** or **Warn**.
It also allows you to set Risky File Types to:

- **Recommended**: This gives you the settings shown in the table of file types below.
- **Allow**: Allows all risky file types.
- **Warn**: Warns the user that a file may be risky before they can download it.
- **Block**: Blocks all risky file types.
- **Let me specify**: This allows you to set a number of individual file types to Allow, Warn, or Block.

### Acceptable web usage

Configure **Acceptable web usage** settings. These control the sites that users are allowed to visit.

**Keep it clean**: Prevents users from accessing adult and other potentially inappropriate websites.

**Gentle guidance**: Blocks inappropriate browsing and warns users before visiting website categories that may impact their productivity.

**Conserve bandwidth**: Blocks inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.

**Business only**: Only allows site categories that are generally business-related.

**Let me specify**: Allows you to configure individual site categories. For each group of categories (such as **Productivity-related categories**) you can set the behavior to Block, Warn, Allow or Let me specify. Choosing Let me specify allows you to configure individual categories within these groups.

For more control over how policy affects websites you can use the **System Settings > Website Management** page.

### Protect against data loss

Select **Protect against data loss** to configure data loss settings.

Selecting this option allows you to choose Block data sharing, Allow data sharing, or Let me specify. Setting these options controls access to web-based email and file downloads.

### Log web control events

Select **Log web control events** to log attempts to visit blocked websites or websites for which we display a warning.

If you do not enable logging, only attempts to visit infected sites will be logged.

### Control sites tagged in Website Management

You can put websites into your own custom categories ("tag" them) and then use a Web Control policy in Sophos Central Admin to control sites in each category.

To set this up, do as follows.

1. In Endpoint: Web Control, go to **Website Management**.
2. Click **Add**.
3. In Add Website Customization, enter a website and add a tag. You can either type in a new tag name, or select a tag you've used before (you'll see suggested tags when you start typing).

4. Click Save.

5. Go to Endpoint Protection in Sophos Central Admin and select the policy you want to use the tag in.

Endpoint: Windows Firewall

You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your computers using a Windows Firewall base policy.

Warning
Other firewalls or your Windows Group Policy settings may affect how the base policy is applied on individual computers. We advise that you test any firewall rules you create (locally or via Group Policy) to make sure that communication with Sophos is allowed.

In Monitor Type, select the level of monitoring you want:

Monitor Only

Devices will report their firewall status to Sophos Central Admin. This is the default option.

Monitor & Configure Network Profiles

Devices will report their firewall status to Sophos Central Admin. You can also choose whether to block or allow inbound connections on Domain Networks, Private Networks and Public Networks. Choose from:

- Block All
- Block (with exceptions): You must set up the exceptions locally on the computer or server. If you don't set up exceptions all inbound connections are blocked.
- Allow All

Server: Application Control

Application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.

We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. In the Controlled Applications list, click Add/Edit List.
   This opens a dialog where you can see the categories of applications that you can control. Sophos supplies and updates the list.

2. Select an application category, for example Browser plug-in.
   A full list of the applications in that category is displayed in the right-hand table.

3. Choose how you want to control applications.
   - Find the applications you want to use and clear the checkbox next to them.
• Click **New applications added to this category by Sophos** (optional). Any new applications that Sophos adds to this category later will automatically be added to your controlled list. Newer versions of applications already in your list will also be added.

4. Click **Save to List** and repeat for each category you want to control.

If you want to control an application that isn't in the list supplied by Sophos, you can ask to have it added. Click the “Application Control Request” link at the bottom of Application Control settings.

5. In **Detection Options**:

• Click **Detect controlled applications when users access them**.

    **Note**
    If you chose to control any new applications added by Sophos, this setting also applies to those new applications.

• Click **Detect controlled applications during scheduled and on-demand scans**.

    Application control uses the scheduled scans and the scanning options (which file types are scanned) that you set in Threat Protection settings.

6. In **Desktop Messaging** you can add a message to the standard notification. If you leave the message box empty only the standard message is shown.

    **Desktop Messaging** is on by default.

    If you switch off **Desktop Messaging** you will not see any notification messages related to Application Control.

    a) Enter the text you want to add.

**Server: Lockdown**

Server Lockdown prevents unauthorized software from running on servers.

To do this, Sophos makes a list of the software already installed, checks it is safe, and allows only that software to run in future.

You lock down a server at its details page.

You can use the Server Lockdown settings in a base policy to change what is allowed without the need to unlock the server. For example, you might want to add and run new software.

**Allowed files/folders**

This option lets you allow software (such as updaters) to run and modify other applications. It also lets you add new software to a locked-down server without unlocking it.

**Warning**

This option “trusts” the software, so that any files it creates or changes are also allowed. This is different from the process when you lock down a server, which only allows the software itself to run.

You can specify files that are allowed, or a folder in which all the files are allowed.
Tip
You can specify a folder where you always download installers for use on the server.

1. Click Add allowed file/folder.
2. Select the type of item to allow (file or folder).
3. Enter the path of the file or folder. You can use the wildcard *.
4. Click Save.

Blocked files/folders

This lets you block software that is currently allowed to run.

You can specify files that are blocked, or a folder in which all the files are blocked.

Tip
You can block a folder used for applications, such as installers, that you want to make available to other users on the network, but don’t want to run on your server.

1. Click Add blocked file/folder.
2. Select the type of item to block (file or folder).
3. Enter the path of the file or folder. You can use the wildcard *.
4. Click Save.

Server: Peripheral Control

Peripheral control lets you control access to peripherals and removable media.

If you need to exempt individual peripherals from that control you should use a Server Peripheral Control Policy in Sophos Central Admin.

Manage Peripherals

In Manage Peripherals, select how you want to control peripherals:

- Monitor but do not block (all peripherals will be allowed): If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you can’t set access rules for them.

- Control access by peripheral type and add exemptions: If you select this, you can go on to set access policies for peripheral types.

Restriction
You can’t add peripheral exemptions at the global level, so you will need to do this at the sub-estate level.
Set Access Policies

Set access policies in the table. The table displays detected peripheral types, the number of each type detected, and the current access policy.

Note
The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

Note
The MTP/PTP category includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:

• **Allow**: Peripherals are not restricted in any way.
• **Block**: Peripherals are not allowed at all.
• **Read Only**: Peripherals can be accessed only for reading.

Note
The **Bluetooth**, **Infrared**, and **Modem** categories do not have the **Read Only** option.

Note
The Wireless Network Adaptor category has a **Block Bridged** option. This prevents bridging of two networks.

Desktop Messaging

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Desktop Messaging** is on by default.

Note
If you switch off **Desktop Messaging** you will not see any notification messages related to peripheral control.

Click in the message box and enter the text you want to add.
Server: Threat Protection

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

Restriction
Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

SophosLabs can independently control which files are scanned. They may add or remove scanning of certain file types in order to provide the best protection.

You can either use the recommended settings or change them.

Intercept X Advanced for Server

If you have this license, your threat protection policy offers protection from ransomware and exploits, signature-free threat detection, and root cause analysis of threat events.

We recommend that you use these settings for maximum protection.

If you enable any of these features, servers assigned to this policy will use an Intercept X Advanced for Server license.

Server Protection default settings

We recommend that you leave these settings turned on. These provide the best protection you can have without complex configuration.

These settings offer:
- Detection of known malware.
- In-the-cloud checks to enable detection of the latest malware known to Sophos.
- Proactive detection of malware that has not been seen before.
- Automatic cleanup of malware.
- Automatic exclusion of activity by known applications from scanning.

Scheduled Scanning

Scheduled scanning performs a scan at a time or times that you specify.

You can select these options:
- **Enable scheduled scan**: This lets you define a time and one or more days when scanning should be performed.

Note
The scheduled scan time is the time on the endpoint computers (not a UTC time).
• **Enable deep scanning:** If you select this option, archives are scanned during scheduled scans. This may increase the system load and make scanning significantly slower.

**Exclusions**

You can exclude files, folders, websites or applications from scanning for threats, as described below.

We’ll still check excluded items for exploits. However, you can stop checking for an exploit that has already been detected (use a **Detected Exploits** exclusion).

Exclusions set in a policy are only used for the users the policy applies to.

**Note**

If you want to apply exclusions to all your users and servers, set up global exclusions on the **Global Settings > Global Exclusions** page.

To create a policy scanning exclusion:

1. Click **Add Exclusion** (on the right of the page).
   
   The **Add Exclusion** dialog is displayed.

2. In the **Exclusion Type** drop-down list, select a type of item to exclude (file or folder, website, potentially unwanted application, or device isolation).

3. Specify the item or items you want to exclude.

4. For **File or folder** exclusions only, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

5. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings, and click **Update**.

**Desktop Messaging**

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Enable Desktop Messaging for Threat Protection** is on by default. If you switch it off you will not see any notification messages related to Threat Protection.

Enter the text you want to add.

**Related concepts**

**Server Protection: Intercept X Advanced** (page 47)
If you have an Intercept X Advanced for Server license, you'll see options in your threat protection policy in addition to the standard Server Protection options.

**Server Protection: Default settings** (page 48)
The server threat protection base policy includes these standard options.
Server Protection: Intercept X Advanced

If you have an Intercept X Advanced for Server license, you'll see options in your threat protection policy in addition to the standard Server Protection options.

Runtime Protection

Restriction
Some options are only available if you have joined the Early Access Program.

Runtime protection protects against threats by detecting suspicious or malicious behavior or traffic on endpoint computers.

- **Protect document files from ransomware (CryptoGuard):** This protects document files against malware that restricts access to files and then demands a fee to release them. You can also choose to protect 64-bit computers against ransomware run from a remote location. You can choose what action you want to take if ransomware is detected. You can terminate any ransomware processes that are running, or you can stop any ransomware processes from writing to the filesystem by isolating them.

- **Protect from master boot record ransomware:** This protects the computer from ransomware that encrypts the master boot record (and so prevents startup) and from attacks that wipe the hard disk.

- **Protect critical functions in web browsers (Safe Browsing):** This protects your web browsers against exploitation by malware.

- **Mitigate exploits in vulnerable applications:** This protects the applications most prone to exploitation by malware. You can select which application types to protect.

- **Advanced exploit mitigation settings:**
  - **Prevent credential theft:** This prevents the theft of passwords and hash information from memory, registry, or hard disk.
  - **Prevent code cave utilisation:** This detects malicious code that's been inserted into another, legitimate application.
  - **Prevent APC violation:** This prevents attacks from using Application Procedure Calls (APC) to run their code.
  - **Prevent privilege escalation:** This prevents attacks from escalating a low-privilege process to higher privileges to access your systems.

  We recommend testing these settings before you apply the policy to your servers.

- **Protect processes:** This helps prevent the hijacking of legitimate applications by malware. You can choose to:
  - protect against process replacement attacks (process hollowing attacks).
  - protect against loading .DLL files from untrusted folders.

- **Enable CPU branch tracing:** CPU malicious code detection is a feature of Intel processors that allows tracing of processor activity for detection. We support it on Intel processors with the following architectures: Nehalem, Westmere, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Goldmont, SkyLake, and Kaby Lake.

  We don't support it if there is a (legitimate) hypervisor on the computer.
Deep Learning

Deep learning uses advanced machine learning to detect threats. It can identify known and previously unknown malware and potentially unwanted applications without using signatures.

Remediation

- **Enable Threat Case creation**: Threat cases let you investigate the chain of events in a malware attack and identify areas where you can improve your security.

- **Allow servers to send data on suspicious files, network events and admin tool activity to Sophos Central**: This sends details of potential threats to Sophos. Ensure it's turned on in any policy for servers where you want to do threat searches.

  **Note**
  This option is available if you have Intercept X Advanced with EDR for Server.

  **Restriction**
  You must turn this option on in both Endpoint and Server Protection to use Intercept X Advanced for Server with EDR.

Server Protection: Default settings

The server threat protection base policy includes these standard options.

We recommend that you leave these settings turned on. These provide the best protection you can have without complex configuration.

**Warning**
Think carefully before you change the recommended settings because doing so may reduce your protection.

**Restriction**
Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

**Restriction**
Some options are only available if you have joined the Early Access Program.

Runtime Protection

Runtime protection protects against threats by detecting suspicious or malicious behavior or traffic.

**Protect network traffic**

- **Detect malicious connections to command and control servers**: This detects traffic between an endpoint computer and a server that indicates a possible attempt to take control of the endpoint computer (a “command and control” attack).
• **Prevent malicious network traffic with packet inspection (IPS):** This scans network communications, identifying and blocking threats before they can harm the operating system or applications.

**Enable Sophos Security Heartbeat:** This sends server “health” reports to each Sophos XG Firewall registered with your Sophos Central account. If more than one firewall is registered, reports go to the nearest one available. If a report shows that a server may be compromised, the firewall can restrict its access.

**AMSI Protection (with enhanced scan for script-based threats).** This protects against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). We scan code forwarded by AMSI before it runs, and we notify the applications used to run the code of threats. If a threat is detected, an event is logged. You can prevent the removal of AMSI registration on your servers.

**Live Protection**

Live Protection checks suspicious files against the latest malware in the SophosLabs database.

**Use Live Protection to check the latest threat information from SophosLabs online:** This checks files during real-time scanning.

• **Use Live Protection during scheduled scans**

**Real-time scanning - Local files and network shares**

Real-time scanning scans files as users attempt to access them and allows access if the file is clean.

**local and remote:** If you select local instead, we don’t scan files in network shares.

**on read:** This scans files when you open them.

**on write:** This scans files when you save them.

**Real-time scanning - Internet**

Real-time scanning scans internet resources as users attempt to access them.

**Scan downloads in progress.**

**Block access to malicious websites:** This denies access to websites that are known to host malware.

**Detect low-reputation files:** This warns if a download has a low reputation. The reputation is based on a file’s source, how often it is downloaded, and other factors. You can specify:

• The **Action to take on low-reputation downloads:** If you select **Prompt user**, users see a warning when they attempt to download a low-reputation file. This is the default setting.

• The **Reputation level:** If you select **Strict**, medium-reputation, as well as low-reputation files, are detected. The default setting is **Recommended**.

**Remediation**

**Automatic cleanup of malware:** This attempts to clean up detected threats automatically. This option is supported on Windows servers and on guest VMs protected by a Sophos security VM (but only if you have installed the Sophos Guest VM Agent on them).
Note
We always clean up PE (Portable Executable) files like applications, libraries, and system files, even if you turn off automatic cleanup. PE files are quarantined and can be restored.

Real-time scanning - Options

Automatically exclude activity by known applications: This prevents Sophos Central from scanning files used by certain widely-used applications. For a list of these applications, see Download Reputation. You can manually exclude activity by other applications by using the Exclusions options.

Detect malicious behavior (HIPS): This protects against threats that are not yet known. It does this by detecting and blocking behavior that is known to be malicious or is suspicious.

Advanced Settings

These settings are for testing or troubleshooting only. We recommend that you leave them set to the defaults.

Server: Update Management

The Update Management base policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

Restriction
Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

Enable Scheduled Updates and select the day and time when you want product updates to become available.
Remember that if computers aren’t on, they won’t get the update until the next time they start.

Server: Web Control

Web Control lets you restrict access to certain categories of website.

Restriction
Web Control settings apply only to Windows servers.

All servers to which this policy applies will use a Server Advanced license.

Website Controls

Select Website Controls to control access to websites that may be inappropriate.
For each website category, you can select:
• Allow: Allows all websites in this category.
• **Warn**: Warns the user that a website may be inappropriate.
• **Block**: Blocks all websites in this category.

**Log web control events**

Click **Log web control events** to log attempts to visit blocked websites or websites for which we display a warning.

If you do not enable logging, only attempts to visit infected sites will be logged.

**Control sites tagged in Website Management**

You can put websites into your own custom categories ("tag" them) and then use a Web Control policy in Sophos Central Admin to control sites in each category.

To set this up, do as follows.

1. For the template that you want to edit, click **Global settings** and then **Website Management**.
2. Click **Add**.
3. In **Add Website Customization**, enter a website, optionally select a category override, and add a tag. You can either type in a new tag name, or select a tag you've used before (you'll see suggested tags when you start typing).
4. Click **Save**.
5. Go to Server Protection in Sophos Central Admin and select the policy you want to use the tag in.

**Server: Windows Firewall**

You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your servers using a Windows Firewall base policy.

You can apply a Windows Firewall base policy to individual servers or to groups of servers.

**Warning**

Other firewalls or your Windows Group Policy settings may affect how the policy is applied on individual servers. We advise that you test any firewall rules you create (locally or via Group Policy) to make sure that communication with Sophos is allowed.

In **Monitor Type**, select the level of monitoring you want.

**Monitor Only**

Servers will report their firewall status to Sophos Central. This is the default option.

**Monitor & Configure Network Profiles**

Servers will report their firewall status to Sophos Central. You can also choose whether to block or allow inbound connections on **Domain Networks**, **Private Networks**, and **Public Networks**.

Choose from:
• **Block All**
• **Block (with exceptions)**: You must set up the exceptions locally on the computer or server. If you don’t set up exceptions all inbound connections are blocked.
• **Allow All**

**Encryption: Device Encryption**

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault on Macs. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

You set up encryption as follows:

1. The Device Encryption agent is installed on Windows computers automatically when you use the standard Windows agent installer (if you have the required license). You must manually install the Device Encryption agent on Macs.
2. Edit a **Device Encryption** base policy and apply the policy to users as described below.
3. Computers are encrypted when those users log in.

**Note**
FileVault encryption is user-based; every user of an endpoint must have encryption turned on.

For full details of how computers are encrypted, see the Sophos Central Device Encryption administrator guide.

**Note**
You can apply device encryption to boot volumes and fixed data volumes, but not to removable media.

To set up a policy:
• Edit a **Device Encryption** base policy
• Open the policy’s **Settings** tab and configure it as described below.

**Settings**

**Device Encryption is on/off**: A computer is encrypted as soon as one of the users the policy applies to logs in.

A Windows endpoint stays encrypted even if a different user who isn’t included in the policy logs in.

**Warning**
You must apply an encryption policy to all users of a specific macOS endpoint to ensure that it is fully protected.

**Encrypt boot volume only**: This option allows you to encrypt the boot volume only. Data volumes are ignored.
Advanced Windows settings

**Require startup authentication**: This option is turned on by default. It enforces authentication via TPM+PIN, passphrase, or USB key. If you turn it off, TPM-only logon protection is installed on supported computers. For more information on authentication methods, see the Sophos Central Device Encryption administrator guide.

**Require new authentication password/PIN from users**: This option is turned off by default. It forces a change of the BitLocker password or PIN after the specified time. An event is logged when users change their password or PIN.

Note
On the endpoint, the feature is only available in Central Device Encryption 2.0 or later.

If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN, an alert is logged.

**Encrypt used space only**: This option is turned off by default. It allows you to encrypt used space only instead of encrypting the whole drive. You can use it to make initial encryption (when the policy is first applied to a computer) much faster.

**Warning**
If you encrypt used space only, deleted data on the computer might not be encrypted, so you should only do this for newly set up computers.

Note
This option does not affect Windows 7 endpoints.

Password protect files for secure sharing (Windows only)

Note
On the endpoint, the feature is only available in Central Device Encryption 2.0 or later.

You can protect files up to 50Mb.

**Enable right-click context menu**: If you turn on this option, a Create password-protected file option is added to the right-click menu of files. Users can attach password-protected files to emails when sending sensitive data to recipients outside your corporate network. Files are wrapped in a new HTML file with encrypted content.

Recipients can open the file by double-clicking it and entering the password. They can send the received file back and protect it with the same or a new password, or they can create a new password-protected file.

**Enable Outlook add-in**: This option adds encryption of email attachments to Outlook. Users can protect attachments by selecting Protect Attachments on the Outlook ribbon. All unprotected attachments are wrapped in a new HTML attachment with encrypted content, and the email is sent.

**Always ask how to proceed with attached files**: If you turn on this option, users must choose how to send attachments whenever the message contains one. They can send them password protected or unprotected.
You can enter excluded domains for which the **Always ask how to proceed with attached files** option does not apply. For example, your organization’s domain. If recipients belong to such a domain, the senders aren’t asked how they want to handle attachments.

Enter only complete domain names and separate them by commas.

**Related information**
Sophos Central Device Encryption administrator guide

**Email Security**

Use this policy to apply security settings to email.

The following settings only apply to inbound messages with the exception of **Enhanced content and file property scan**, which applies to both inbound and outbound messages.

**Spam Filtering**

Each email message is analyzed and given a spam score. The higher the score the more likely the message is to be spam. Messages with the highest spam scores are rated as **Confirmed Spam**.

Messages are categorized based on their spam score and you can choose how the categories are processed. Messages are split into:

- **Confirmed Spam**: These are messages that conform to known and verified spam patterns.
- **Bulk**: These are solicited messages sent using mass mailing, for example newsletters sent to a mailing list.
- **Suspected Spam**: These are messages that have been identified as suspicious.

For each category choose an action.

The default settings are:

- **Confirmed Spam**: Quarantine
- **Bulk**: Quarantine
- **Suspected Spam**: Deliver

**End-user message settings**

When you turn on **Smart banners**, a banner is displayed at the top of inbound email messages to show if the email is trusted.

**Note**

Smart banners are only inserted when emails are received from outside the organization. If an internal employee forwards such an email to another internal employee, the banner remains in the forwarded email.

Emails from Sophos, for example **Quarantine Summary** emails, will not display banners.
CAUTION
We strongly recommend that you route outbound email through Sophos Central before you turn on smart banners. If you don’t, external recipients see the banner in replies or forwarded email and can modify end-user allow and block lists.

You can turn on and off the following banner types:

- **Trusted**: The email was sent from an allowed sender and passed DNS authentication (SPF, DKIM, or DMARC).
- **Unknown**: The email was sent from outside your organization.
- **Untrusted**: The email was sent from outside your organization and failed DNS authentication (SPF, DKIM, or DMARC).

Quarantine Settings

You can choose to send a quarantine summary message to each protected mailbox. The message contains a table containing spam messages that were quarantined since the last summary message was sent. You can schedule when the messages are sent.

Users can release or delete quarantined spam messages by clicking the appropriate link in the quarantine summary message.

To set up quarantine summary messages:

1. Turn on **Send a quarantine summary email**.
2. Select when you want the messages sent.

   **Tip**
   All days are selected by default. Click a day to deselect it.

3. One time slot is shown by default. You can add up to three more by clicking **Add another time**. To delete a time slot, click the delete icon next to it.

   **Note**
   The default time slot can’t be deleted.

Sender Check

Sender checks allow you to verify whether an email originates from where it claims to come from. Email Security uses **DMARC**, **DKIM**, and **Header anomalies** checks to do this. Sender checks are performed in the order they appear in the UI. If an email fails the first sender check, the other checks are not carried out.

You can override the sender checks by adding domains and email addresses to the **Allow** list.

**DMARC** (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication policy and reporting protocol. It builds on the DKIM and SPF protocols to detect and prevent email spoofing. You can control what happens to messages that fail DMARC checks.

Select from:
• **Conform to sender policy**: What happens to the message depends on what the sender stated in their DMARC policy. (This is the default value.)

• **Tag subject line**: Email Security adds a tag to the message’s subject line indicating that it is a spoofed message.

• **Quarantine**: Message is quarantined.

• **Reject**: Message is rejected.

• **Deliver**: Sends the message to the mail server for delivery.

**DKIM** (DomainKeys Identified Mail) is an authentication framework used to sign and validate a message based on the domain of the sender. You can control what happens to messages that fail DKIM checks.

Select from:

• **Tag subject line**: Email Security adds a tag to the message's subject line indicating that it is a spoofed message. (This is the default value.)

• **Quarantine**: Message is quarantined.

• **Reject**: Message is rejected.

• **Deliver**: Sends the message to the mail server for delivery.

The **Header anomalies** check identifies email that appears to come from your own domain but originates from an external domain by checking the from header of the email against the recipient domain, and the from address in the envelope.

• If the domain in the from address matches the recipient's domain, the mail is considered to be spoofed.

• If the from address in the header is different to the from address in the envelope, the mail is considered to be spoofed.

**Note**
The header needs to match both the criteria above to trigger the **Header anomalies** check.

You can control what happens to messages that fail the **Header anomalies** check.

Select from:

• **Tag subject line**: Email Security adds a tag to the message’s subject line indicating that it is a spoofed message. (This is the default value.)

• **Quarantine**: Message is quarantined.

• **Reject**: Message is rejected.

• **Deliver**: Sends the message to the mail server for delivery.

**Enhanced Email Malware Scan**

**Enhanced content and file property scan**: This is our highest level of protection against email malware. It is on by default.

This setting applies to inbound and outbound messages.

**Note**
If malware is detected in a message, it is always discarded.
**Un-scanned emails**: You can choose what happens to messages that cannot be scanned. The available actions are:

- **Quarantine**
- **Delete**
- **Tag subject line**

This setting applies to inbound messages only.

**Time of Click URL Protection** *(Email Advanced license only)*: When Time of Click URL Protection is enabled, URLs contained within inbound messages are rewritten so that they point to Sophos Email instead of the original destination.

When the link is clicked, Sophos Email performs an SXL lookup, and if it is malicious it is blocked. If the URL is clean, the action taken when you click the link will depend on what you have specified in the policy. For example, if you have set medium risk websites as allowed, once the link has been checked and has been classified as not malicious, the link will take you to the original link destination.

The domain name will be displayed at the start of the rewritten URL so that you can see where the link will send you, if allowed. For example `d=domain.com`.

You can select the action you want to take for websites with the following reputation levels:

- **High risk**: Includes illegal sites, sites containing malware and phishing sites.
- **Medium risk**: Includes sites associated with spam and anonymizing proxies.
- **Unverified**: The reputation of the website can't be verified.

You can't allow high risk websites.

**Note**

You can also control whether URLs are rewritten in plain text messages and within securely signed messages:

- **Plain text messages**: refers to emails with no HTML formatting. Without HTML formatting, when URL rewriting is enabled, the entire encoded URL will display in the email. You can bypass URL rewriting in these messages by deselecting the **Re-write URLs in plain text messages** option.

- **Securely signed messages**: URL rewriting may break the signatures of S/MIME, PGP, and DKIM signed messages. You can bypass URL re-writing in these messages by deselecting the **Re-write URLs within securely signed messages** option.

**CAUTION**

Please use caution if you choose to bypass URL re-writes, as URLs in these messages will not be protected.

**Sandstorm** *(Email Advanced license only)*: Sandstorm sends emails that may contain active malicious content to an isolated virtual environment where they are opened and checked. If emails are found to be malicious, they are removed.

When Sandstorm is enabled, you can select your preferred sandbox location.
**Tip**
Select **Let Sophos decide (recommended)** to automatically route messages for optimal performance.

Messages that may be malicious will run in a virtual environment for closer inspection.

Messages that are clean are delivered as normal. Messages that contain advanced threats are discarded.

**Impersonation Protection (Email Advanced license only):** This feature detects emails that pretend to be from well-known brands, or from very important people (VIPs) in your organization. Choose the action taken when emails are detected by this feature. In summary reports, these emails are labeled as advanced threat. You can add email addresses for VIPs in **VIP management**.

**Related information**
Sophos Sandstorm
knowledge base article 117936
10 Deployment

You can install Sophos Endpoint Protection on Windows computers (or servers) and Macs for any of your sub-estates.

Download an installer and create an installation script for each sub-estate, as follows:

1. Go to Deployment.
2. Download the installer for the operating system you want to protect.
3. Download the CSV file. You’ll use this to specify the products to install and other details needed for this sub-estate.
4. Use the installer and CSV file to create your installation script.
   The CSV file includes only sub-estates that have a valid endpoint product license.
5. Use the script.

Tip
You must use the CSV file. The installer won’t work without it.

Related information
Installer precheck messages

10.1 Installer command-line options for Windows

You can use the following command-line options with the Sophos Central Endpoint installer for Windows.

Command-line options

These options apply to:
- Sophos Endpoint Advanced 11.5.11 and later.
- Sophos Endpoint Standard 11.5.11 and later.

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>No proxy detection</td>
<td>--noproxydetection</td>
<td>Doesn't attempt to perform automatic proxy detection.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>No competitor removal</td>
<td>-- nocompetitorremoval</td>
<td>Doesn't attempt to automatically remove competitors. (Only on installation of Sophos Anti-Virus.)</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>-- language=&lt;language ID&gt;</td>
<td>Allows you to manually set the installer language. By default the installer uses the system language.</td>
<td>Language ID</td>
</tr>
<tr>
<td>Group</td>
<td>-- devicegroup=&lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to.</td>
<td>A group to join. If it doesn't exist, it is created.</td>
</tr>
<tr>
<td>CRT catalog path</td>
<td>-- crtcatalogpath=&lt;path to CRT catalog&gt;</td>
<td>Allows you to specify your own catalog of competitors to remove.</td>
<td>Full path and filename to catalog folder. Example: -- crtcatalogpath=C:\catalog \productcatalog.xml.</td>
</tr>
<tr>
<td>Message relays</td>
<td>-- messagerelays=&lt;comma-separated message relay list of IPs including the port&gt;</td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port 8190. Example: -- messagerelays=IPADDRESS:8190.</td>
</tr>
<tr>
<td>Proxy address</td>
<td>-- proxyaddress=&lt;custom proxy address&gt;</td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (will use HTTPS)</td>
</tr>
<tr>
<td>Proxy username</td>
<td>-- proxyusername=&lt;custom proxy user name&gt;</td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username of the proxy.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>-- proxypassword=&lt;custom proxy password&gt;</td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td>Computer name override</td>
<td>-- computernameoverride=&lt;override for computer name&gt;</td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Computer description</td>
<td>-- computerdescriptionoverride=&lt;override for description&gt;</td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td>override</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain name override</td>
<td>-- domainnameoverride=&lt;override for domain&gt;</td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer token</td>
<td>-- customertoken=&lt;the customer token&gt;</td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Products to install       | -- products=<comma-separated list of products>                               | Specifies a list of products to install. If you specify a product that you don't have a license for, then it isn't installed. | A list of products to install, comma-separated.
<p>|                           |                                                                              |                                                                            | Available options are: antivirus, intercept, mdr, deviceEncryption or all. |</p>
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Example usage</strong></th>
<th><strong>Description</strong></th>
<th><strong>Trailing argument</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local install source</td>
<td><code>--localinstallsource=&lt;path-to-install-source&gt;</code></td>
<td>Specifies a local install source to use during installation. This allows an installation to occur without having to download the installer files.</td>
<td>It isn't necessary to populate the local install source, but it is necessary to create a <code>SophosLocalInstallSource</code> folder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If an empty folder is provided it is populated during the first installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you wish to pre-populate the cache you can take a copy of the files from an already installed endpoint or from your update cache:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>%ProgramData\Sophos\AutoUpdate\data\Warehouse</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>%ProgramData\Sophos\UpdateCache\www\warehouse</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Even if a populated local install source is provided, internet access is still required and some files are downloaded. The amount of data downloaded depends on various factors including, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Whether the platform of the installation endpoint differs from the files already populated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Whether the warehouse has changes since the local install source was populated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For the purpose of this example <code>SomeContent</code> represents the files and folders within the Warehouse folder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you wish to pre-populate the cache you can take a copy of the files from an already installed endpoint or from your update cache:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>%ProgramData\Sophos\AutoUpdate\data\Warehouse</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>%ProgramData\Sophos\UpdateCache\www\warehouse</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Even if a populated local install source is provided, internet access is still required and some files are downloaded. The amount of data downloaded depends on various factors including, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Whether the platform of the installation endpoint differs from the files already populated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Whether the warehouse has changes since the local install source was populated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For the purpose of this example <code>SomeContent</code> represents the files and folders within the Warehouse folder.</td>
</tr>
</tbody>
</table>
### Option Example usage Description Trailing argument

| Message trail logging | --traillogging | Turns on the logging of message content between the endpoint and Sophos Central during installation. You must switch this option off after installing, see Enabling a diagnostic message trail of Sophos MCS. | |

**Note**

There is no command-line option for installation from an update cache. The installer automatically assesses connectivity to any update caches set up in the Sophos Central account and installs from them.

### Windows examples

**Install Sophos Anti-Virus and Intercept X without user interaction:**

SophosSetup.exe --products=antivirus,intercept --quiet

**Install using a proxy:**

SophosSetup.exe --proxyaddress=<ProxyIP/FQDN>:<Port>

**Install using a message relay:**

SophosSetup.exe --messagerelays=192.168.10.100:8190

### Language IDs

<table>
<thead>
<tr>
<th>Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1033</td>
</tr>
<tr>
<td>French</td>
<td>1036</td>
</tr>
<tr>
<td>German</td>
<td>1031</td>
</tr>
<tr>
<td>Japanese</td>
<td>1041</td>
</tr>
<tr>
<td>Spanish</td>
<td>1034</td>
</tr>
<tr>
<td>Italian</td>
<td>1040</td>
</tr>
<tr>
<td>Polish</td>
<td>1045</td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>1046</td>
</tr>
</tbody>
</table>
### Related information

- Enabling a diagnostic message trail of Sophos MCS
- Domains and ports required for communication to and from Sophos Central Admin and the Sophos Central managed endpoint
- Frequently Asked Questions (FAQs)
- New endpoint installer frequently asked questions
- An Internet connection could not be established
- Installer precheck messages

### 10.2 Installer command-line options for Mac

The Sophos Central Endpoint installer for Mac supports the following command-line options.

#### Mac command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet --install</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>--devicegroup &lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to.</td>
<td>A group to join. If it doesn’t exist, it is created.</td>
</tr>
<tr>
<td>Message relays</td>
<td>--messagerelays &lt;space-separated message relay list of IPs including the port&gt;</td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port, 8190.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: --messagerelays IPADDRESS:8190 IPADDRESS:8190</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Proxy address</td>
<td>--proxyaddress <code>&lt;custom proxy address&gt;</code></td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (uses HTTPS).</td>
</tr>
<tr>
<td>Proxy port</td>
<td>--proxypoint <code>&lt;proxy port&gt;</code></td>
<td>Specifies a port that the proxy uses.</td>
<td>Port for the proxy.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>--proxyusername <code>&lt;custom proxy user name&gt;</code></td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username for the proxy.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>--proxypassword <code>&lt;custom proxy password&gt;</code></td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td>Computer name override</td>
<td>--computernameoverride <code>&lt;override for computer name&gt;</code></td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td>Computer description override</td>
<td>--computerdescriptionoverride <code>&lt;override for description&gt;</code></td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td>Domain name override</td>
<td>--domainnameoverride <code>&lt;override for domain&gt;</code></td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td>Preferred domain name for usernames in Sophos Central</td>
<td>--mcsPreferredDomainName</td>
<td>Sets the client to send usernames as domain\username instead of machine \username.</td>
<td></td>
</tr>
<tr>
<td>Registration server</td>
<td>--mgmtserver <code>&lt;registration server URL&gt;</code></td>
<td>Specifies the MCS server to connect to.</td>
<td>MCS server URL.</td>
</tr>
<tr>
<td>Customer token</td>
<td>--customertoken <code>&lt;the customer token&gt;</code></td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Products to install</td>
<td>--products &lt;space separated list of products to install&gt;</td>
<td>Specifies a list of products to install. If you specify a product that you don't have a license for, then it isn't installed.</td>
<td>A list of products to install, space-separated. Available options are: antivirus, intercept, deviceEncryption or all.</td>
</tr>
</tbody>
</table>

**Note**

The Mac installer is aware of all the message relays and update caches when the installation is downloaded. Changes to caches and relays mean that you need to download a new installation. You can specify relays using the command line as well.

**Mac examples**

Install Sophos Anti-Virus and Intercept X without user interaction:

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --products antivirus intercept --quiet
```

Install using a proxy:

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --proxyaddress <ProxyIP/FQDN> --proxyport <Port>
```

Install using a message relay:

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --messagerelays 192.168.10.100:8190
```

**Related information**

Installer precheck messages
11 Explore Products

On the Explore Products page, you can learn about extra products you can add to Sophos Central Admin.
12 Global Security News

On the Global Security News page, you can view current security news articles.
13 Account Details

The **Account Details** page lets you manage your enterprise account. You can manage your licensing.

If you are a Super Admin you can switch off Enterprise Management.

To access this page, click your account name in the upper right of the user interface and select **Account Details**.

13.1 Account Preferences

The **Account Preferences** page lets you switch off enterprise management.

To access this page, select your account name in the upper right of the user interface and select **Account Preferences**.

Enterprise management

**Restriction**
You can only switch off enterprise management if you are a Super Admin.

There are restrictions on switching off enterprise management:

- All sub-estates must have an administrator with the Super Admin role.
- Your enterprise can't have master licensing enabled.
- Your enterprise can't be in the process of converting to master licensing.

What happens to the enterprise administrators?

- All enterprise administrators are logged out.
- All Enterprise Super Admins that enabled enterprise management are given the Super Admin role for their Sophos Central Admin account.
- All other enterprise administrators are deleted. You can add them later as administrators in the appropriate Sophos Central Admin account.

Switch off Enterprise management

To switch off Enterprise management:

1. Select **Disable enterprise management**.
2. Review the information in **Confirm disable** and select the acknowledgment option.
3. Select **Disable enterprise**.
13.2 Licensing

You can activate and manage your Sophos licenses.

Click your account name (upper right of the user interface), select **Licensing**.

License Management Type

Here you can see how your licenses are managed.

- **Enterprise Master Licenses**: Licenses are managed at enterprise level and shared between all the sub-estates managed by the enterprise.
- **Sub-Estate Licenses**: Licenses are managed at the sub-estate level. You can only use these licenses within the sub-estate. To see the licensing details go to Sub-Estates.

You can't turn off **Enterprise Master Licenses** once you've selected it.

**Note**

You can only activate and manage your licenses here if you are using **Enterprise Master Licenses**.

Buy a license

You can buy licenses through your partner. Select **Buy Licenses** to go to a page where you can sign up for licenses.

View end-user license agreement

Click this link to display the Sophos End User License Agreement in a separate window. If you want to print it, press Ctrl+P.

View your licenses and usage

A list shows your current license(s), with the following details for each license.

- **License**: The name of the license you purchased.
- **Type**: The type of license you have.

**Note**

Trial Licenses belong to sub-estates.

- **Usage**: The number of users or servers using this license.
- **Limit**: The maximum number of users or servers that can use this license. The limit depends on the subscription.
- **Expires**: The date when the license expires.
• **License ID**: License number.

**Related tasks**

Activate a license (page 71)
You can activate a new license on the **Licensing** page.

### 13.2.1 Activate a license

You can activate a new license on the **Licensing** page.

You can also activate an upgraded license there if necessary. Some upgraded licenses are activated automatically.

1. Ensure you have the license key shown in the License Schedule that Sophos sent you.
2. Enter your key.
   - If you see **Apply Activation Key**, enter your key and click **Apply**.
   - If you see an **Apply license key** link, select it. Enter the key and select **Apply**.
3. If your account already has licenses for the features included on the key, you see another dialog. This lets you choose how to use your new licenses.
   - **Renew** starts the new licenses when your current licenses expire.
   - **Change** starts the new licenses now. We'll adjust the license term so that all your licenses expire on the same date.

   Click **Apply** again.

**How the "Change" option works**

An enterprise administrator orders 50 licenses for one year. Six months later, they place another order for 50 licenses for one year.

If the enterprise administrator selects **Change**, we do as follows:

- Add the new licenses to the older ones. The enterprise administrator now has 100 licenses.
- Add the remaining time on the older licenses (50 x 6 = 300 sub-estate months) to the time on the new licenses (50 x 12 = 600 sub-estate months). The total is 900 sub-estate months.
- Distribute the time over all 100 licenses. Each sub-estate license now runs for 9 months from the date when the key was applied (and the expiry date is adjusted accordingly).

The enterprise administrator now has 100 licenses that will all expire 9 months from now.

In most cases the existing license expiry date gets extended but do check the new expiry date shown.
13.3 Enterprise Master Licenses

You can opt to manage your licenses at enterprise level. Your licenses are shared between the sub-estates managed by your enterprise. You cannot turn off Enterprise Master Licenses once you have changed license management.

Introduction

If your organization has a single Sophos Central Admin account that owns all the purchased (full) licenses you can transfer the licenses to your Sophos Central Enterprise account. These licenses are the master licenses for your entire organization. Follow the license transfer instructions.

If you have several sub-estates with independent licensing you need to consolidate your licenses to use them as master licenses. Follow the consolidation instructions.

Enterprise Super Admins can allocate licenses from the pool of master licenses.

License allocation

If you don't allocate licenses, a sub-estate can use any license from the pool of available licenses.

If you set the license allocation for a sub-estate to zero for a specific license type, the sub-estate can't use licenses of that type from your pool. The product isn't available to that sub-estate.

If you allocate licenses of a specific type to a sub-estate, the sub-estate can use those licenses.

If a sub-estate uses licenses over its allocation for a license type this shows as over-usage for the enterprise, as well as the sub-estate.

You can change license allocation at any time.

If a license expires or if you renew with a different number of licenses, your allocations don't update automatically.

If you unlink or delete a sub-estate, their licenses revert to the pool of available licenses.

Transfer licenses

Before you begin:

- You must have only one sub-estate that owns all your full licenses.
- You must have Enterprise Management turned on in the sub-estate that owns the licenses.

When you transfer:

- You cannot go back to using individual licenses for each sub-estate.
- All licenses are shared across the sub-estates in your enterprise.
- You must manage licenses in Sophos Central Enterprise.
- The Sophos Central administrators for your organization can't buy licenses or apply activation keys in Sophos Central Admin.

To transfer your licenses:

1. Click your account name (upper right of the user interface) and select Licensing.
2. Click **Convert to Enterprise Master Licenses**.
3. Read the confirmation message about conversion and click **Convert to Enterprise Master Licenses**.

All your licenses are moved to your Sophos Central Enterprise account. Your licenses are shown in the **Licensing** page.

Any of your sub-estates that are using trial licenses are converted to full licenses.

All your sub-estates now use licenses from your master licensing pool.

---

**Consolidate licenses**

You need to get a new activation key that consolidates your licenses. In most cases this key is applied automatically. You may receive a key from your partner. If you do, you need to apply it on the **Licensing** page.

**Before you begin:**

- You must have several sub-estates with independent licenses.
- You must have Enterprise Management turned on for one of the sub-estates.

**When you consolidate:**

- License consolidation may take a few days.
- You cannot go back to using individual licenses for each-sub-estate.
- All licenses are shared across the sub-estates in your enterprise.
- You must manage all licenses in Sophos Central Enterprise.
- The Sophos Central administrators for your organization can't buy licenses or apply activation keys in Sophos Central Admin.

**To consolidate your licenses:**

1. Click your account name (upper right of the user interface) and select **Licensing**.
2. Click **Convert to Enterprise Master Licenses**.
3. Read the confirmation message about conversion and click **Convert to Enterprise Master Licenses**.
   
   The **Licensing** page now shows that you have requested conversion to master licenses.
   
   A consolidation request email is sent to you and your Sophos partner.
4. Work with your Sophos partner to create a consolidation plan.
5. Your new activation key may be applied automatically. If not, enter the key in **Apply consolidation enterprise licenses activation key** and click **Apply**.

All your licenses are moved to your Sophos Central Enterprise account. Your licenses are shown in the **Licensing** page.

Any of your sub-estates that are using trial licenses are converted to full licenses.

All your sub-estates now use licenses from your master licensing pool.
14 Supported Web Browsers

The following browsers are currently supported.

- Microsoft Internet Explorer 11 and Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (Mac only).

We recommend that you install or upgrade to a supported version in the above list and that you always run an up-to-date version. We aim to support the latest version and previous version of Google Chrome, Mozilla Firefox, and Apple Safari. If an unsupported browser is detected you will be redirected to https://central.sophos.com/unsupported.

Note
Sophos Central Enterprise is not supported on mobile devices.
15 Get additional help

To get help from Sophos Support:
1. Click Help in the top right of the user interface and select Create Support Ticket.
2. Fill in the form. Be as precise as possible so that Support can help you effectively.
3. Optionally, select the option to enable Support to directly access your Sophos Central session to be better able to help you.
4. Click Send.

Sophos will contact you within 24 hours.

Note
If you selected the option to enable Support to access your Sophos Central session, this function is enabled when you click Send. Remote assistance will automatically be disabled after 72 hours. To disable it sooner, click on your account name (upper right of the user interface), select Account Details, and click the Sophos Support tab.

Submit feedback

To submit feedback or a suggestion to Sophos Support:
1. Click Help in the top right of the user interface and select Give Feedback.
2. Fill in the form.
3. Click Submit.

Additional help

You can also find technical support as follows:

• Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.

16 Legal notices

Copyright © 2020 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.