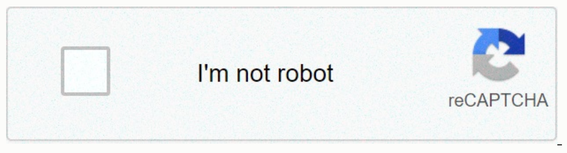

Continue

Mimecast administration console guide

This document describes the SAAS application workflow's SAML identity provider configuration by using the SAAS application template. To configure Mimecast (Admin), follow these steps: Log on to the BIG-IP user interface, and then click Select Category Federation. Select the SAML identity provider for the SAAS application to configure BIG-IP as an SAML identity provider. Review the required configuration information and complete the following action before configuring the SaaS application: Enter identity provider data. Enter the configuration details for the virtual server. You configure the authentication method that you use for the SAML identity provider. After you receive the application configuration confgure, configure the (optional) endpoint control and customization settings. The Saas app displays a list of apps from which you can choose to configure applications from your SAML service provider. Select a specific application and click Add. For example, to configure Mimecast (Admin), select Mimecast (Admin), and then click Add. Specify an application name. The system uses the name internally to identify the application configuration details and the SAML service provider for it. Select whether the application supports IDP-initiated requests. Select IdP initiated to display an application resource at the top of the web. Specify or change the caption. The Web tip uses a caption to display an application resource. Specify an optional description for the application. To configure Mimecast (Admin) to provide the following inputs: Account code: ACCOUNTCODE is your unique Mimecast account code as specified in administration | Account '|'. Administration Console Area Account Settings page: Select the Mimecast grid area that hosts your organization's Mimecast account. You configure all additional attribute values to include saml approval in the SaaS application. Each SAML property has a property name and attribute value. Session variable values can specify attribute values. Configure the AD or LDAP query to include specific properties in session variables. Configure additional approval for consumer service URI if the application requires such URI. Specify whether to sign the confirmation and response, and specify the signing algorithm. Specify whether you want to request a signed authentication request. If necessary, select the signing certificate. Specify whether you want to encrypt the approvals. If necessary, specify the encryption algorithm and select the encryption certificate. To complete the workflow configuration, configure optional endpoint checks and customizations. Configuration deployment on the Summary screen. To retrieve metadata for this configuration, go to . Select the SAML SSO object created by Mimecast (Admin), and then click Export Metadata. You can use exported IdP SAML metadata to configure the Mimecast (Admin) service for the IdP provider configuration. For information about the Mimecast (Admin) documentation, see SAML To test the configuration, click click to test the configuration on the Summary page. When you log on successfully, you should see a web peak that contains applications initiated by the IdP. ×Sorry interrupt the CSS Error basic mimecast guide. Mimecast is a cloud-based e-mail filtering and archiving service. Email security is an important part of many businesses, and Mimecast provides users with additional security against threats such as viruses and phishing and spam reduction. The service also has options for archiving and consistency; this allows companies to ensure access to email is still available during the outage of their email server. If you have chosen to use Mimecast, you will repoint your domain mail exchanger (MX) entries to the Mimecast server cluster, and you will be granted access to a Web portal known as the Mimecast Management Console. It is intended as the main driver of mimecast features and the portal used to manage it. If you have a broader problem with your email in general, why not read our handy email troubleshooting guide here. Set up your email server IP address in the Log On Mimecast Administration Console and navigate to Gateway à Policies à Delivery routing. On the right side, click Definitions next to Delivery routing. Click New Route Definition to set up a new delivery route. To edit an existing one, click the record. Set the Hostname field to the FQDN IP address of your e-mail server. Enable or block the sender To add a new blocked or enabled sender at the Mimecast account level, do the following: Log on to the Mimecast Administration Console Go to Directories – > Groups, on the left, click Blocked Senders or Allowed Senders. This is a domain-level policy that is run before the end-user's individual policy. White List Sender's IP Address in Mimecast Sometimes you may need to enable an IP address via Mimecast, it may be preferable to a white record by domain or email address under certain conditions. To add an IP address to the token list: Open gateway – > Policies. In the Allowed senders list, locate and click it. If there is a policy for the allowed IP addresses, there is a record that says it applies to Everyone and All, if you click it and look at the Validity section at the bottom, you may see existing whitelist IP addresses. If this is the case, you can add additional required IP addresses to the validity section here. If all and all policies are not defined to allow senders, do the following: Click New Policy. In the Policy narrative box, enter an easily understandable name, such as Allowed IP addresses. Under Sender-enabled policy, select Allow sender. Select All emails as sender and E-mail messages. select the Override Policy check box. Add the IP addresses that are required in the Source IP Ranges field by using CIDR characters. For example: To add one IP address: 222.111.111.222/32 22.111.111.0/32 To add an address range 22.111.111.0/24 Adding and assigning new Mimecast administrator users Existing mimecast administrator users can assign the administrator role to other system users and, if necessary, add new users. Log on to the Mimecast Administration Console. Then go to Directories -> Internal. Then, click the domain needed. To edit an existing user, you can use the search feature, and then click to change the role assigned to the user. Click RoleEdit and click the role you want to assign. Then click Add to User Role. You can add more than one new user to the role here. If you want to add a new user, you must do so by using the New Address option in Directories -> Internal - > domain.com screen. However, if you use Active Directory Server, new mimecast users are automatically added to AD. Use only the New Address function to add non-AD users. You can then change the role of the new user by following the other steps above. The sensitivity level of mimecast pornographic image recognition functionality can be changed to suit your needs. Mimecast Administration Console Logon: Go to the -> Policy gateway, then definitions –> attachment sets Click new attachment collection definition Here you can increase or decrease the number of images above n% probability. The smaller the selected percentage, the greater the probability of filtering the image. Select smaller amounts to filter more content. Select larger amounts to allow more content. Notification options are useful for informing users when a message is blocked. For example, if you have a group of IT users, you can also add them for notification. Registering a targeted threat protection device After TTP is activated, the default settings require users to register their device to pass through links and emails. All this is done automatically. e-mail – The user sends an e-mail to sign up and they follow the links to register the device. However, some users may encounter problems where Mimecast will ask them to sign up repeatedly, even if they have done so in the past. A useful KB article on this issue is here: This feature works on a cookie basis and continue to work effectively, after the device is registered the resulting cookie must be stored and stored in the browser. This poses a number of problems because many companies have group policies that delete cookies every time the browser is closed. Devices, such as smartphones, also have this clear feature setup by default. Mimecast has had only a few complaints about this and in cases where the policy of the IT group cannot be changed, Mimecast has suggested that customers have turned it off. Device registration can be turned off and TTP is still working perfectly. How the system works is that the email sspcious URL gets blocked, end users can know the email to say that they click on the link and then have to enter their email address in the code sent to them, which they then enter the URL provided. It is designed as a shield for a 2-step authentication type, but as noted above, this second step is entirely on cookies, and cookies pose security risks and problems. You can remove this step so that the end user only has to click a link that resembles how it works when spam emails are blocked to release an email message. To turn off the need to register devices, go to Account > Account settings > User access and permissions, and then clear the Targeted threat protection authentication check box. Open the Relay error message is not allowed. A common error message that may appear when you mark mimecast non-delivery errors is: Reason: Open relay is not allowed. To get over this, you need to add the destination domain to the allowed list to transfer by: Services > Directories > Profile Groups > Relay then add to the list from the Create as for other policies. Mimecast Digest Reporting, which enables the Digest Notification feature, may help Mimecast end-users find emails that are filtered and stored for various reasons within the Mimecast Management Portal. End-users can release e-mail messages directly if necessary. Log on to the Mimecast Administration Portal and navigate to Services > Gateway > Policies, and then select the definitions for the digest kits policy. Then select the definitions specified on the next screen, which are probably called the definition of the default level of the setting. You can select the type of emails you want to see e-mail to contain, for example, all junk e-mail, attachment policy emails, or any content filtering that is in hand. You can also choose when you want end users to receive a digestive email. If you have configured it if you want, click Save. To activate it, make sure that there is a policy setup. To achieve this, it will move back to the policy list as described above, but this time just click somewhere in the Digest Sets line, not the Definitions button. There should be a policy that looks something like this: If not, select New Policy and setup standard policy as you normally do, with parameters valid from everyone, valid internal addresses, and Digest Set the name you have defined above. When a user receives a digestive report, they see three options next to each e-mail message in the report— / Block / Enable. Clicking Unlock, releases the email immediately and delivers it to the user. The Block option returns to sender, and all future emails from the same sender are automatically rejected. The Enable option releases the email message and also adds the sender to the whitelist. For more information about this feature, see the Help link for the Mimecast Portal. Malicious content to get through Mimecast Legacy MS Office files is known to send malicious attachments through Mimecast from time to time. A certain breed of these attachments are malicious content and macros in MS Office files such as Word and Excel documents. Especially older versions of MS Office files are easier to hide things. Since most people do not use the old version of MS Office, Mimecast has developed a shield to help prevent these problematic legacy MS Office files. It can be activated by going to Services > Gateway > Policies > Attachment Management Definitions > Default Attachment Sets > Block Dangerous File Types. This takes you to the policy properties screen, and the required setting is: Finding an email on the Mimecast portal This may seem obvious to some, but it's a common question about the portal. The most efficient and fastest way to find an email with any description, be it delivered, rejected or whatever, navigate to Services > Gateway > Tracking option, and not an accepted email option that only queries the email that Mimecast has agreed to process. If Tracking is not on the Gateway menu, account settings are probably configured for 0 days to keep the log, which is not unusual. In this case, ask your technical support team. Call us on 0845 625 9025 or contact us for more information about how we can help you with email security. Security.