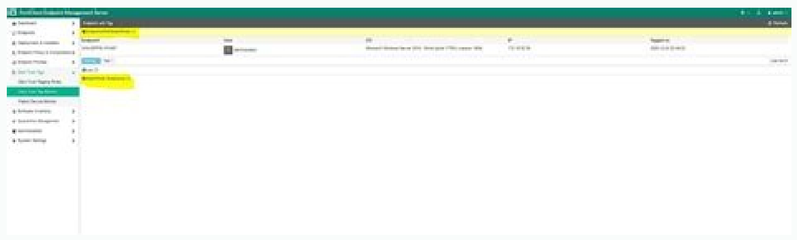
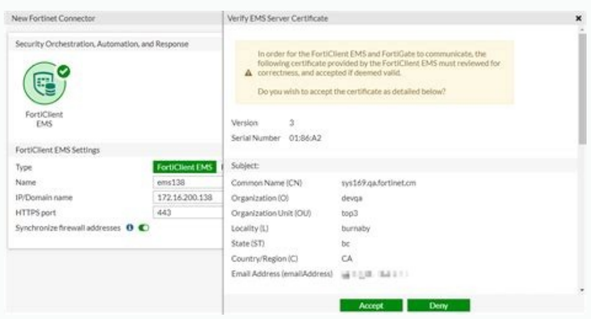
Forticlient ems 6. 0 admin guide





Forticlient ems administration guide 6.4. Forticlient ems admin guide. Fortinet ems admin guide.

You can use FortiClient EMS to deploy FortiClient on endpoints. Deploying FortiClient from FortiClient EMS requires the following steps: After you deploy FortiClient on endpoints and endpoints connect to FortiClient EMS, you can update endpoints by editing the associated profiles. You can also use FortiClient EMS to uninstall and upgrade FortiClient on endpoints. You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient installs on endpoints and endpoints connect to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints. You cannot use FortiClient EMS to deploy an initial installation of FortiClient (macOS) to endpoints. However, after FortiClient (macOS) is installed on endpoints and endpoints connect to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient (macOS) on endpoints. CUITANDOKTER.COM - Home forticlient 6-2-1 administration guide 6-2-1 microsoft windows the following instructions guide you though the installation of forticlient on a microsoft windows computer- for more information see the forticlient windows release notes- to check forticlient s - This is an index of images Administration Guide Forticlient 6 2 1 Fortinet greatest By simply using syntax we possibly can 1 Article into as many completely readers friendly editions as you like that individuals say to and indicate Writing stories is a lot of fun for your requirements. Most of us obtain amazing a great deal of Nice article Administration Guide Forticlient 6 2 1 Fortinet beautiful image however many of us simply present your articles that we believe include the ideal images.Your images Administration Guide Forticlient 6 2 1 Fortinet is merely with regard to beautiful demonstration when you such as the reading remember to purchase the authentic articles. Help your creator simply by buying the first sentences Administration Guide Forticlient 6 2 1 Fortinet and so the admin can offer the most effective image and also go on doing work Here at looking for offer all sorts of residential and commercial work. you have to make your search to get your free quotation hope you are okay have a good day. Administration Guide Forticlient 6 2 1 Fortinet Documentation Library Home forticlient 6.2.1 administration guide 6.2.1 microsoft windows the following instructions guide you though the installation of forticlient on a microsoft windows computer. for more information, see the forticlient (windows) release notes. to check forticlient 's .... Home forticlient 6.2.1 administration guide introduction forticlient is an all in one comprehensive endpoint security solution that extends the power of fortinet's advanced threat protection .... Administration Guide Forticlient 6 2 1 Fortinet Documentation Library . Oct 10, 1990 · home forticlient 6.2.1 administration guide copy link connecting vpns before logging on (ad environments) the vpn tag holds global information controlling vpn states. the vpn .... The setup process is as follows. the ems administrator completes some actions, and the endpoint user completes others. the administrator configures a forticlient deployment package in ems. the administrator specifies which modules to install in the deployment package. the administrator prepares to deploy forticlient .... Administration Guide Forticlient 6 2 6 Fortinet Documentation Library Fortiems | Basic Installation And Configuration | Migration Ems | Forticlient Part1 this is series of video tutorial of basic installation and configuration of fortiems and forticlient . first two part of the video initial in this video i'm going to install and license fortinet enterprise management server (ems) and configure multiple forticlient environment vsphere 6.7 forticlient ems 7.0.0 fortigate 6.4.2 fortigate 7.0.1 not working fortigate 6.4.6 not working import if you want a mass deployment of #forticlient, then #forticlientems is a perfect tool for you. stay tuned! in this video, i will show you some options to deploy #forticlient to windows machines by using #forticlientems 7.0. in this video, you will learn what forticlient ems is and how to connect forticlient ems to active directory and integrate it with the in this fortinet tutorial video, learn how to setup a fortigate firewall courtesy of firewalls managed services network environment windows 2016 hyper v fgt vm64 hv v7.0.1 build0157 fortinet.out.hyperv.zip this video provides a quick startup guide to ems 7.0, showing what needs to be configured to begin using the ems. for detailed firewall #fortigate #paloalto fortigate firewall administration full course in 3 hours. a high level overview is necessary on the fortimanager and fortianalyzer before you dive in to each. they have large concepts a lot of people access their fortigates remotely without the proper precautions and consideration being executed. these five tips Next Monitor FortiClient connections Previous Configure FortiClient profiles When FortiClient Telemetry connects to FortiGate/EMS, the user's AD domain name and group are both sent to FortiGate/EMS. Administrators may configure the FortiGate/EMS to deploy endpoint and/or firewall profiles based on the end user's AD domain group. The following steps are discussed in more details: l Configure users and groups on AD servers l Configure FortiAuthenticator l Configure FortiGate/EMS l Connect FortiClient Telemetry to FortiGate/EMS l Monitor FortiClient connections Configure users and groups on AD servers Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time. Configure FortiAuthenticator Configure FortiAuthenticator to use the AD server that you created. For more information see the FortiAuthenticator Administration Guide in the Fortinet Document Library. Configure FortiGate/EMS FortiGate Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO): Go to User& Device > Single Sign-On. Select Create New in the toolbar. The New Single Sign-On Server window opens. In the type field, select Fortinet Single-Sign-On Agent. Telemetry connections with AD user groups Enter the information required for the agent. This includes the name, primary and secondary IP addresses, and passwords. Select an LDAP server in the drop-down list if applicable. Select More FSSO agents to add up to three additional agents. Select OK to save the agent configuration. Create a user group: Go to User& Device > UserGroups. Select Create New in the toolbar. The New UserGroup window opens. In the type field, select Fortinet Single-Sign-On (FSSO). Select members from the drop-down list. Select OK to save the group configuration. Configure the FortiClient profile: Go to Security Profiles > FortiClient Profiles. Select Create New in the toolbar. The New FortiClient Profile window opens. Enter a profile name and optional comments. In the Assign Profile To drop-down list select the FSSO user group(s). Configure FortiClient configuration as required. Select OK to save the new FortiClient profile. Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who connect successfully, but have no matching FortiClient profile. Configure the firewall policy: Configure the firewall policy as described in Configure firewall policies on page 35. Ensure that Compliant with FortiClient Profile is selected in the policy. EMS Add a new domain: Under the Endpoints heading, in the Domains section, select Add a new domain. The Domain Settings window opens. Enter the domain information as required. Select Test to confirm functionality, then, if successful, select Save to add the domain. The domain's organizational units (OUs) will automatically be populated in the Domains section under the Endpoints heading. For more information, see the FortiClient EMS Administration Guide, available in the Fortinet Document Library. Connect FortiClient Telemetry to FortiGate/EMS The Microsoft Windows system on which FortiClient is installed should join the domain of the AD server configured earlier. Users may log in with their domain user name. Configure FortiClient Telemetry connections with AD user groups Following this, FortiClient endpoint connections will send the logged-in user's name and domain to the FortiGate/EMS. The FortiGate/EMS will assign the appropriate profiles based on the configurations. Next Roaming clients (multiple redundant gateways) Previous Configure FortiClient Telemetry connections with AD user groups The following FortiOS CLI command lists information about connected clients. This includes domain-related details for the client (if any). diagnose endpoint record-list Record #1: IP_Address = 172.172.172.111(1) MAC_Address = b0:ac:6f:70:e0:a0 Host MAC_Address = b0:ac:6f:70:e0:a0 MAC list = b0-ac-6f-70-e0-a0; VDOM = root Registration status: Forticlient installed but not registered Online status: offline DHCP on-net status: off-net DHCP server: None FCC connection handle: 6 FortiClient version: 5.1.29 AVDB version: 22.137 FortiClient app signature version: 3.0 FortiClient vulnerability scan engine version: 1.258 FortiClient feature version status: 0 FortiClient UID: BE6B76C509DB4CF3A8CB942AED2064A0 (0) FortiClient config dirty: 1:1:1 FortiClient KA interval dirty: 0 FortiClient Full KA interval dirty: 0 FortiClient server config: d9f86534f03fbed109676ee49f6cfc09:: FortiClient config: 1 FortiClient iOS server mconf: FortiClient iOS mconf: FortiClient iOS server ipsec_vpn mconf: FortiClient iOS ipsec_vpn mconf: Endpoint Profile: Documentation Reg record pos: 0 Auth_AD_groups: Auth_group: Auth_user: Host_Name: OS_Version: Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601) Host_Description: AT/AT COMPATIBLE Domain: Last_Login_User: FortiClient_User_Name Host_Model: Studio 1558 Host_Manufacturer: Dell Inc. CPU_Model: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz Memory_Size: 6144 Installed features: 55 Enabled features: 21 online records: 0; offline records: 1 status — none: 0; uninstalled: 0; unregistered: 1; registered: 0; blocked: 0 Roaming clients (multiple redundant gateways) Next FortiClient Provisioning Previous Monitor FortiClient connections The following figure illustrates three corporate FortiGate networks. Each FortiGate can reach each other over a WAN network. FortiClient can only reach one FortiGate at a time. FortiClient may connect directly to the FortiGate or through a NAT device. If FortiClient connects through a NAT device to the FortiGate, do not enforce endpoint control compliance on the FortiGate. On each of the three FortiGate devices configure the following: l Interface IP addresses l FortiClient profile l Device identification in the interface l FortiClient profile in the applicable firewall policy l Endpoint control synchronization Endpoint control synchronization allows you to synchronize endpoint control for multiple FortiGate devices. To enable endpoint control synchronization via the CLI enter the following commands on your FortiGate: config endpoint-control forticlient-registration-sync edit 1 set peer-ip 172.20.52.19 next edit 2 set peer-ip 172.22.53.29 end end Roaming clients (multiple redundant gateways) The IP addresses set for the peer-ip field are the WAN IP addresses for each of the FortiGate devices in the synchronization group. You need to add the following XML configuration to FortiClient for this synchronization group. Modify the configuration file to add the following: Corporate Network 10.18.51.9;10.20.52.19;10.22.53.29 The IP addresses are the internal IP addresses for each of the three FortiGates in the synchronization group. FortiClient can reach any of these IPs, one at a time. If the three FortiGate devices share the same DNS name, use the following XML configuration: Fortinet Americas fct_americas.fortinet.com The DNS server should return one reachable FortiGate IP address for the domain name used. You will need to manually add FortiClient to the synchronization group when FortiClient initially connects with the FortiGate. Once added, no further action is required. On your FortiGate, use the following CLI command to list all connected FortiClient endpoints: diagnose endpoint registration list registered-forticlients FortiClient #1 (0): UID = BE6B76C509DB4CF3A8CB942AED200000 vdom = root status = registered registering time = Fri May 2 15:00:07 2014 registration expiry time = none source IP = 172.172.172.111 source MAC = b0:ac:6f:70:e0:a0 user = user host OS = Microsoft Windows 7 , 64-bit restored registration = no remote registration = yes registration FGT = FGT60C3G11000000 Total number of licences: 10 Total number of granted licenses: 1 Total number of available licences: 9 Roaming clients (multiple redundant gateways) The remote registration entry indicates whether this specific FortiClient is connected to this FortiGate, or to another FortiGate within the synchronization group. If any of the FortiGate devices require a password to complete connection, you can use the following XML configuration to provide password information to FortiClient: Corporate Network 10.18.51.9;10.20.52.19;10.22.53.29 uNbre@kab1e Next Install FortiClient as part of cloned disk images Previous Roaming clients (multiple redundant gateways) FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems by using Microsoft Active Directory (AD). You can use FortiClient EMS to deply FortiClient to multiple Microsoft Windows systems. For information, see the FortiClient EMS Administration Guide. This chapter contains the following sections: l Install FortiClient on computers l Install FortiClient on infected systems l Install FortiClient as part of cloned disk images l Deploy FortiClient using Microsoft Active Directory servers For information on customizing your FortiClient installation, see Custom FortiClient Installations. Download FortiClient installation files The FortiClient installation files can be downloaded from the following sites: Fortinet Customer Service & Support: Requires a support account with a valid support contract. Download either the Microsoft Windows (32-bit/64bit) or the Mac OS X installation file. FortiClient homepage: forticlient.com Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient. Download the FortiClient online installation file. On this page you can download the latest version of FortiClient for Microsoft Windows and Mac OS X, and link to the iOS, and Android versions. Install FortiClient on computers The following section describes how to install FortiClient on a computer that is running a Microsoft Windows or Apple Mac operating system. Microsoft Windows computer The following instructions will guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the FortiClient (Windows)Release Notes. When installing FortiClient, it is recommended to use the FortiClientOnlineInstaller file. This file will launch the FortiClient Virus Cleaner which will scan the target system prior to installing the FortiClient application. Install on computers To check the digital signature of FortiClient, right-click on the installation file and select Properties. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details. To install FortiClient (Windows): Double-click the FortiClient executable file. The Setup Wizard When using the FortiClient Online Installer file, the FortiClient Virus Cleaner will run before launching the Setup Wizard. If a virus is found that prevents the infected system from downloading the new FortiClient package, see Install FortiClient on infected systems on page 47. In the Welcome screen, read the license agreement, select the Yes, I have read and accept the license checkbox, and select Next to continue. The Choose Setup Type screen is displayed. You can read the license agreement by clicking the License Agreement button. You have the option to print the EULA in this License Agreement screen. Select one of the following setup types: l Complete: All Endpoint Security and VPN components will be installed. l VPN Only: Only VPN components (IPsec and SSL) will be installed. Install FortiClient on computers Select Next to continue. The Destination Folder screen is displayed. Select Change to choose an alternate folder destination for installation. Select Next to continue. FortiClient will search the target system for other installed antivirus software. If found, FortiClient will display the Conflicting Antivirus Software page. You can either exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient real-time protection disabled. This dialog box is displayed during a new installation of FortiClient and when upgrading from an older version of FortiClient, which does not have the antivirus feature installed. It is recommended to uninstall the conflicting antivirus software before installing FortiClient or enabling the antivirus real-time protection feature. Alternatively, you can disable the antivirus feature of the conflicting software. Select Next to continue. Select Install to begin the installation. Select Finish to exit the FortiClient Setup Wizard. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select Yes to restart your system now, or select No to manually restart later. FortiClient will update signatures and components from the FortiGuard Distribution Network (FDN). FortiClient will attempt to connect FortiClient Telemetry to the FortiGate. If the FortiGate cannot be located on the network, manually connect FortiClient Telemetry. See Connect FortiClient Telemetry manually on page 54. To launch FortiClient, double-click the desktop shortcut icon. Microsoft Server You can install FortiClient on a Microsoft Windows Server 2008 R2, 2012, or 2012 R2 server. You can use the regular FortiClient Windows image for Server installations. Please refer to the Microsoft knowledge base for caveats on installing antivirus software in a server environment. See the Microsoft Anti-Virus exclusion list: Install on infected systems Mac OS X computer The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the FortiClient (Mac OS X)Release Notes. To install FortiClient (Mac OS X): Double-click the FortiClient .dmg installer file to launch the FortiClient installer. The FortiClient Installer will install FortiClient on your computer. Select Continue. Select the lock icon in the upper right corner to view certificate details. Read the Software License Agreement and select Continue. You have the option to print or save the Software Agreement in this window. You will be prompted to Agree with the terms of the license agreement. Select the destination folder for the installation. Select Install to perform a standard installation on this computer. You can change the install location from this screen. Depending on your system, you may be prompted to enter your system password. After the installation completes successfully, select Close to exit the installer. FortiClient has been saved to the Applications Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon in the FortiClient console to make changes to the FortiClient configuration. Install FortiClient on infected systems The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual. Any virus found during this step is quarantined before installation continues. In case a virus on an infected system prevents downloading of the new FortiClient package, use the following process: Install FortiClient as part of cloned disk images Boot into "safe mode with networking" (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network). Run the FortiClient installer. This scans the entire file system. A log file is generated in the logs sub-directory. If a virus is found, it will be quarantined. When complete, reboot back into normal mode and run the FortiClient installer to complete the installation. Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message will be generated. It is necessary to reboot back into normal mode to complete the installation. Next Deploy FortiClient using Microsoft Active Directory servers Previous FortiClient Provisioning If you configure computers using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier. This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application will generate its own unique identifier the first time the computer is started. To include a FortiClient installation in a hard disk image: Install and configure the FortiClient application to suit your requirements. You can use a standard or a customized installation package. Right-click the FortiClient icon in the system tray and select Shutdown FortiClient. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights. Shut down the computer. Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on. Create the hard disk image and deploy it as needed. Next Deploy FortiClient using EMS Previous Install FortiClient as part of cloned disk images There are multiple ways to deploy FortiClient to endpoint devices including using Microsoft Active Directory (AD). Deploy using EMS The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different. Using Microsoft AD to deploy FortiClient: On your domain controller, create a distribution point. Log on to the server computer as an administrator. Create a shared network folder where the FortiClient MSI installer file will be distributed from. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder. Select Start > Administrative Tools > Active Directory Users and Computers. After selecting your domain, right-click to select a new Organizational Unit (OU). Move all the computers you wish to distribute the FortiClient software to into the newly-created OU. Select Start > Administrative Tools > Group Policy Management The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, Select Create a GPO in this domain, and Link it here. Give the new GPO a name then select OK. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select Edit. The Group Policy Management Editor MMC Snap-in will open. Expand ComputerConfiguration > Policies > Software Settings. Right-click Software Settings and select New > Package. Select the path of your distribution point and FortiClient installer file and then select Open. Select Assigned and select OK. The package will then be generated. If you wish to expedite the installation process, on both the server and client computers, force a GPO update. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then. Uninstall FortiClient using Microsoft Active Directory server: On your domain controller, select Start > Administrative Tools > Group Policy Management. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select Edit. The Group Policy Management Editor will open. Select ComputerConfiguration > Policy > Software Settings > Software Installation. You will now be able to see the package that was used to install FortiClient. Right-click the package, select All Tasks > Remove. Choose Immediately uninstall the software from users and computers, or Allow users to continue to use the software but prevent new installations. Select OK. The package will delete. If you wish to expedite the uninstall process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then. Next FortiClient Telemetry Connection Previous Deploy FortiClient using Microsoft Active Directory servers You can use FortiClient EMS to deploy FortiClient (Windows) in managed mode to devices in your network that are running a supported Windows operating system. For installation information, see the FortiClient Upgrade FortiClient EMS Administration Guide. An upgrade schedule dialog box is displayed in advance when deploying FortiClient from EMS to endpoints running Windows operating system. If no FortiClient is installed on the endpoint, no reboot is required for the installation, and no upgrade schedule dialog box is displayed. The user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog box is displayed with a 15 minute warning. Upgrade FortiClient For information about supported upgrade paths for FortiClient, see the FortiClient Release Notes. Previous Deploy FortiClient using EMS In managed mode, FortiClient uses a gateway IP address to connect FortiClient Telemetry to FortiGate or FortiClient EMS. For more information, see Telemetry Gateway IP Lists on page 31. How FortiClient locates FortiGate/EMS FortiClient uses the following methods in the following order to automatically locate FortiGate/EMS for Telemetry connection: Telemetry Gateway IP List FortiClient Telemetry searches for IP addresses in its subnet in the Gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system. If FortiClient cannot find any FortiGates in its subnet, it will attempt to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the Gateway IP list. Remembered gateway IP list You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate/EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate/EMS. Default gateway IP address The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connection to EMS. FortiClient obtains the default gateway IP address from the operating system on the endpoint device. The default gateway IP address of the endpoint device should be the IP address for the FortiGate interface with Telemetry enabled. If FortiClient is unable to automatically locate a FortiGate/EMS on the network for Telemetry connection, you can use the following methods to manually connect Telemetry to FortiGate/EMS: l Type the gateway IP address of FortiGate/EMS. See Connect FortiClient Telemetry manually on page 54. FortiClient uses the same process to connect Telemetry to FortiGate/EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change. Telemetry Connection Connect FortiClient Telemetry after installation Connect FortiClient Telemetry after installation After FortiClient software installation completes on an endpoint, FortiClient automatically launches and searches for a FortiGate or FortiClient EMS for FortiClient Telemetry connection. See also How FortiClient locates FortiGate/EMS on page 51. When FortiClient locates a FortiGate or EMS, the FortiGate Detected or Enterprise Management Server (EMS) Detected dialog box is displayed. The following options are availble: Endpoint User Displays the name of the endpoint user that is logged into the endpoint device. Logged into Domain Displays the name of domain if applicable. Hostname Displays the name of the endpoint device. Profile Details Click to display details of the profile that FortiClient will download after you accept connection to FortiGate/EMS. See also FortiClient profiles on page 29. Remember this FortiGate Select for FortiClient to remember the gateway IP address of the FortiGate/EMS to which you are connecting Telemetry. See also Remember gateway IP addresses on page 52. Click Accept to connect FortiClient Telemetry to the identified FortiGate/EMS. Alternately, you can click Cancel to launch FortiClient software without connecting FortiClient Telemetry. FortiClient launches in standalone mode. You can manually connect FortiClient Telemetry later. After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient downloads a profile from FortiGate/EMS. A system tray bubble message will be displayed once the profile download is complete. Remember gateway IP addresses When you confirm Telemetry connection to a FortiGate/EMS, you can instruct FortiClient to remember the gateway IP address of the FortiGate/EMS. If a connection key is required, FortiClient remembers the connection password too. FortiClient can remember up to 20 gateway IP addresses for FortiGate/EMS. 52 Remember gateway IP addresses FortiClient Telemetry Connection The remembered IP addresses display in the Local Gateway IP list. FortiClient can use the remembered gateway IP addresses to automatically connect to FortiGate/EMS. See also Forget gateway IP addresses on page 60. To remember FortiGate/EMS: In the FortiGate/EMS Detected dialog box, select the Rememberthis FortiGate or Rememberthis EMS (not shown) check box. Click Accept. FortiClient remembers the IP address and password, if applicable. Previous FortiClient Telemetry Connection The Compliance tab displays whether FortiClient Telemetry is connected to FortiGate or EMS. When FortiClient Telemetry is connected to FortiGate, the Compliance tab displays whether FortiClient and the endpoint device are compliant with the compliance rules defined by FortiGate. When FortiClient and/or the endpoint device are not compliant, the Compliance tab displays information about how FortiClient and the endpoint device can be returned to a status of compliant. You can also use the Compliance tab to connect FortiClient Telemetry to FortiGate/EMS and disconnect FortiClient Telemetry from FortiGate/EMS. Enable compliance For FortiClient in standalone mode, the Compliance tab is not used. For FortiClient in managed mode, an administrator enables and disables endpoint compliance by using FortiGate. When endpoint compliance is enabled, FortiClient must be installed on endpoint devices, and FortiClient Telemetry must be connected to FortiGate. When FortiClient Telemetry is connected, the FortiClient endpoint receives a profile from FortiGate that contains the compliance rules and optionally some FortiClient configuration information. If FortiGate is integrated with EMS, the FortiClient endpoint might also receive a profile from EMS that contains FortiClient configuration information. Connect FortiClient Telemetry manually On endpoints, FortiClient Telemetry must be connected to FortiGate to use the compliance feature. Alternately, FortiClient Telemetry can be connected to EMS, but you cannot use the compliance feature when FortiClient Telemetry is connected to EMS. If FortiClient Telemetry was not automatically connected after FortiClient installation, you can manually connect FortiClient Telemetry to FortiGate/EMS. To manually connect FortiClient Telemetry: Go to the Compliance In the FortiGate IP box, type the IP address or URL of FortiGate or EMS, and click Connect. FortiClient Telemetry connects to FortiGate/EMS, FortiClient downloads a profile from FortiGate/EMS. Disconnect FortiClient Telemetry You must disconnect FortiClient Telemetry from FortiGate/EMS to connect to another FortiGate/EMS or to uninstall FortiClient. To disconnect FortiClient Telemetry: On the Compliance tab, click the Click to Disconnect A confirmation dialog box is displayed. Click Yes to disconnect FortiClient from FortiGate/EMS. After you disconnect FortiClient Telemetry from FortiGate/EMS, FortiClient Telemetry automatically connects with the FortiGate/EMS when you re-join the network. See also Forget gateway IP addresses on page 60. View compliance status Information available on the Compliance tab depends on whether FortiClient is running in standalone mode or managed mode. In managed mode, the information displayed on the Compliance tab also depends on whether FortiClient Telemetry is connected to FortiGate or FortiClient EMS. When FortiClient Telemetry is connected to EMS and the feature is enabled in EMS, a picture of the endpoint user might display on the Compliance tab. FortiClient displays the picture that is defined for the Windows operating system on the endpoint device. If FortiClient cannot find a picture defined for the Windows operating system on the endpoint device, no picture is displayed on the Compliance tab. Standalone mode When FortiClient is running in standalone mode, the Compliance tab is not used. The Compliance tab is labeled Not Participating. The unlocked icon at the bottom left of the screen indicates that settings in FortiClient console are unlocked, and the endpoint user can change them. If you want to use the compliance feature, you must connect FortiClient Telemetry to FortiGate. View compliance The Compliance tab displays the following information: FortiGate IP Type the IP address or URL of FortiGate/EMS, and click Connect to connect FortiClient Telemetry. Unlocked icon Indicates that the settings in FortiClient console are unlocked and can be changed. FortiClient Telemetry connected to EMS When FortiClient Telemetry is connected to EMS, compliance is not enforced. The Compliance tab is labeled Connected to EMS. The locked icon at the bottom left of the screen indicates that settings in the FortiClient console are locked by EMS. EMS controls the settings by pushing a profile to FortiClient. The Compliance tab displays the following information: Compliance status Indicates that the compliance

enforcement feature requires FortiClient Telemetry connection to FortiGate. FortiClient EMS information Displays the name and IP address of the EMS to which FortiClient Telemetry is connected. You can disconnect by clicking the Click to Disconnect link, view details about the endpoint device by clicking the View Details link, and view the gateway IP list that FortiClient is using for FortiClient Telemetry connection by clicking the Show IP List That This FortiClient is Sending Telemetry Data to link. FortiClient Telemetry information Displays how often FortiClient Telemetry communicates with FortiClient EMS and when the next communication will occur. FortiClient Telemetry also downloads FortiClient configuration information from EMS. Locked icon Indicates that the settings in FortiClient console are locked by EMS. You can change the settings by using a profile in EMS. FortiClient Telemetry connected to FortiGate When FortiClient Telemetry is connected to FortiGate, network access compliance is enforced. The locked icon at the bottom left of the screen indicates one of the following statuses: The settings in the FortiClient console are locked by the profile from EMS. In this case, FortiGate is integrated with EMS, and the non-compliance action in FortiGate is set to block or warn. FortiGate provides the compliance rules, and EMS provides the profile of FortiClient settings. The settings in the FortiClient console are unlocked. In this case, FortiGate provides the compliance rules, and the non-compliance action in FortiGate is set to auto-update. You can change the FortiClient settings unrelated to the compliance rules. In the following example, FortiClient Telemetry is connected to FortiGate, but EMS provides the profile of FortiClient settings. The settings are locked by EMS. In the following example, FortiClient Telemetry is connected to FortiGate, and a profile is not provided by EMS. The settings are locked by FortiGate. View compliance The Compliance tab displays the following information: Compliance status Displays the compliance status of the computer on which FortiClient is installed. The computer is either in compliance or not compliant with FortiGate. FortiGate information Displays the name and IP address of the FortiGate to which FortiClient Telemetry is connected. You can perform the following actions: l Disconnect FortiClient Telemetry by clicking the Click to Disconnect link l View details about the endpoint device by clicking the View Details link l View compliance rules from FortiGate by clicking the Show Compliance Rules From link l View the gateway IP list being used for FortiClient Telemetry connection by clicking the Show IP List That This FortiClient is Sending Telemetry Data to link. FortiClient Telemetry information Displays how often FortiClient Telemetry communicates with FortiGate and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and FortiGate, sending status information to FortiGate and receiving network-access rules and possibly some FortiClient configuration information from FortiGate. When FortiGate is integrated with EMS, notification information is also sent to EMS. Depending on the FortiGate settings, EMS might also send FortiClient configuration information to FortiClient. Monitoring Displays whether the endpoint is monitored by EMS. Locked or unlocked icon Indicates whether the settings in FortiClient console are locked or unlocked. View user details You can view user details when FortiClient is compliant with FortiGate rules. You cannot view user details when FortiClient is not compliant with FortiGate rules. To view user details: On the Compliance tab, view the name of the user beside the View Details Click the View Details link to view the following information: Online/offline Displays whether the endpoint device is online or offline. A green icon indicates the endpoint is online. Off-Net/On-Net Displays whether the endpoint device is on-net or off-net. A green On-Net icon indicates the endpoint is on-net. Username Displays the name of the user logged into FortiClient on the endpoint. Hostname Displays the name of the device on which FortiClient is installed. Domain Displays the name of the domain to which the endpoint device is connected, if applicable. Click the X to close the dialog box. View gateway IP lists You can view the following gateway IP lists in FortiClient: The Gateway IP list is created by administrators. Endpoint users cannot change the list. For more information, see Telemetry Gateway IP Lists on page 31. The Local Gateway IP list is created by endpoint users. It is the list of remembered FortiGate/EMS devices. When FortiClient Telemetry is connected for the first time, you can choose to remember the gateway IP address. See Remember gateway IP addresses on page 52. The gateway IP lists are used to automatically connect FortiClient Telemetry to FortiGate/EMS. To view gateway IP lists: On the Compliance tab, click the Show IP List That This FortiClient is Sending Telemetry Data to The Gateway IP List and the Local Gateway IP List are displayed. Fix not compliant Click X to close the list. Forget gateway IP addresses When you instruct FortiClient to forget an IP address for FortiGate/EMS, FortiClient Telemetry will not use the IP address to automatically connect to FortiGate/EMS when re-joining the network. To forget FortiGate/EMS: On the Compliance tab, click the Show IP List That This FortiClient is Sending Telemetry Data to In the Local Gateway IP List, click Forget beside the gateway IP addresses that you no longer want FortiClient to remember. Click X to close the list. Fix not compliant status You can maintain compliance by ensuring that FortiClient software is configured to meet the requirements specified in the compliance rules defined by the FortiGate to which FortiClient Telemetry is connected. FortiGate might also require the endpoint device to run a specific version of FortiClient or operating system software. When FortiClient displays a status of Not-Compliant, you can take actions that will make FortiClient compliant with FortiGate again. View not-compliant status When a FortiClient endpoint does not comply with the FortiGate compliance rules, the Compliance tab displays a status of Not-Compliant. Fix not compliant The following information is displayed on the Compliance tab: This computer is Not Compliant with Displays the name and IP address of the FortiGate to which FortiClient Telemetry is connected. You can view the compliance rules by clicking the Show Compliance Rules from link. Vulnerability Scan Displays critical vulnerabilities found for the endpoint when detected. You must fix the critical vulnerabilities to return to compliant status by clicking Fix Now. You can also click the Details link to view details about the vulnerabilities. Software Out of Date Displays whether FortiClient software is outdated. You must upgrade to the specified FortiClient version to return to compliant status by clicking Update Now. System Compliant Displays whether the operating system of the endpoint complies with FortiGate rules. You must use the specified operating system to return to compliant status. You can view the allowed operating systems by clicking the Details link. Fix All Click to fix all reported issues. This option is available when the non-compliance setting in FortiGate is set to block or warn, and EMS has not provided a profile to the FortiClient endpoint. This option is not available when the non-compliance setting in FortiGate is set to auto-update. If the Fix All link is not displayed, contact your administrator to help adjust the FortiClient Console and computer settings to remain in compliance with FortiGate. View compliance rules When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the settings required on FortiClient console for the FortiClient endpoint to remain compliant. Fix not compliant To view compliance rules: On the Compliance tab, click the Show Compliance Rules From The compliance rules from FortiGate are displayed. Click Close to return to the Compliance Fix now Issues that caused a not-compliant status can be fixed to return FortiClient endpoints to a compliant status. When available, you can click the Update Now, Fix Now, or Fix All links on the Compliance tab to return FortiClient endpoints to compliant status. When FortiClient has a not compliant status and the Update Now, Fix Now, or Fix All links are not displayed, endpoint users should contact their system administrator for help with configuring the endpoint and FortiClient Console to remain in compliance with FortiGate. What links are available depend on the configuration of FortiGate and EMS. The following table summarizes when links are available: Configuration Compliance Rules FortiClient Configuration Options FortiGate Yes No FortiClient settings are unlocked. Click Update Now, Fix Now, and Fix All links when available. View notifications Configuration Compliance Rules FortiClient Configuration Options FortiGate integrated with EMS Yes No FortiClient settings are unlocked. Click Update Now, Fix Now, and Fix All links when available. Yes Yes FortiClient settings are locked by EMS. Use EMS to update the profile that contains the FortiClient configuration to meet the requirements of the compliance rules. To fix now: On the Compliance tab, perform one of the following options: l Click Fix All. l Click Update Now. l Click Fix Now. The non-compliance issues are fixed, and the FortiClient endpoint returns to a status of compliant. If the Fix All, Update Now, or Fix Now links are not displayed on the Compliance tab, contact your system administrator for help with changing the endpoint and FortiClient Console settings. Examples of blocked FortiClient endpoints FortiClient endpoint access to the network can be blocked a number of ways. The following table provides examples of how FortiClient endpoints can be blocked from accessing the network and how to regain access. Configuration Failure Blocked By Solution Endpoint control is enabled on FortiGate. FortiClient Telemetry is connected to FortiGate. FortiClient configuration fails to meet the com- pliance rules specified by FortiGate FortiClient View the Compliance tab in FortiClient console, and follow the instructions to configure FortiClient to meet the compliance rules specified by FortiGate. Endpoint control is enabled on FortiGate. FortiClient Telemetry is not connected to FortiGate. FortiClient Telemetry is not connected FortiGate In FortiClient console, connect FortiClient Telemetry to FortiGate. View notifications Select the notifications icon in the FortiClient console to view notifications. When a virus has been detected, the notifications icon will change from gray to yellow. Event notifications include: View notifications Antivirus events including scheduled scans and detected malware. l Endpoint Control events including configuration updates received from FortiGate. WebFilter events including blocked web site access attempts. l System events including signature and engine updates and software upgrades. Select the Threat Detected link to view quarantined files, site violations, and real-time protection events. To view notifications: In FortiClient Console, click the Notifications icon in the top-right corner. The list of notifications is displayed. Click Close to close the list. Next Web Security/Web Filter FortiClient includes an antivirus module to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient will also scan for and remove rootkits. In FortiClient, file-based malware, malicious websites, phishing, and spam URL protection are part of the antivirus module. Scanning can also be extended by using FortiSandbox. Enable/disable realtime protection For FortiClient in standalone mode, you can enable and disable realtime protection by using the FortiClient console. For FortiClient in managed mode, an administrator enables, disables, and configures realtime protection by using a FortiClient profile. See FortiClient profiles on page 29. Enable/disable Antivirus This setting can only be configured when FortiClient is in standalone mode. To enable Antivirus: On the AntiVirus tab, click the settings icon next to Realtime Protection Disabled. The real-time protection settings page opens. Select the Scan files as they are downloaded orcopied to my system check box. Click OK. If you have another antivirus program installed on your system, FortiClient will show a warning that your system may lock up due to conflicts between different antivirus products. Conflicting antivirus warning To disable antivirus: On the AntiVirus tab, click the settings icon next to Realtime Protection Enable. The real-time protection settings page opens. Enable/disable realtime protection Clear the Scan files as they are downloaded orcopied to my system check box, and click OK. Enable/disable FortiSandbox This setting can only be configured when FortiClient is in standalone mode. FortiClient integration with FortiSandbox allows you to submit files to FortiSandbox for automatic scanning. When configured, FortiClient will send supported files downloaded over the internet to FortiSandbox if they cannot be detected by the local, real-time scanning. Access to the downloaded file is blocked until the scanning result is returned. As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all real-time and on-demand AV scanning. You cannot configure this option when FortiClient is connected to FortiGate/EMS. The administrator configures this option on FortiGate/EMS. To enable FortiSandbox: On the AntiVirus tab, select the settings icon to open the real-time protection settings page. Select Extend scanning using FortiSandbox. Enter the FortiSandbox IP address, then select Test to ensure that the connection is correct. Scan and analysis on demand Set the remaining options as needed. Click OK to apply your changes. Next Application Firewall Web Security/Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FortiGuard Distribution Network (FDN). You can create a custom URL filter exclusion list which overrides the FDN category. When a FortiClient endpoint is connected to FortiGate/EMS, the Web Security tab becomes the Web Filter tab in the FortiClient console. Enable/disable Web Security/Web Filter For FortiClient in standalone mode, you can enable, disable, and configure web security by using the FortiClient console. You can define what sites are allowed, blocked, or monitored, and you can view violations. For FortiClient in managed mode, an administrator enables, disables, and configures Web Filter by using a FortiClient profile. See FortiClient profiles on page 29. Enable/disable Web Security This setting can only be configured when FortiClient is in standalone mode. To enable or disable Web Security: On the Web Security tab, toggle the Enable/Disable link in the FortiClient console. Web Security is enabled by default. The following options are available: Enable/Disable Select to enable or disable Web Security. Configure Web Security profiles X Violations (In the Last 7 Days) Select to view Web Security log entries of the violations that have occurred in the last 7 days. Settings Select to configure the Web Security profile, exclusion list, and settings, and to view violations. Enable/disable Web Filter This setting can only be configured when FortiClient is in managed mode. When FortiClient is connected to a FortiGate/EMS, the Web Security tab will become the Web Filter tab. A FortiClient profile can include a Web Filter profile from a FortiGate or EMS. On a FortiGate device, the overall process is as follows: l Create a Web Filter profile on the FortiGate, l Add the Web Filter profile to the FortiClient Profile on the FortiGate. On EMS, web filtering is part of the endpoint profile. Configure Web Security profiles This setting can only be configured when FortiClient is in standalone mode. You can configure a Web Security profile to allow, block, warn, or monitor web traffic based on website categories and sub-categories. Edit Web Security exclusion lists Web Security/Web Filter To configure web security profiles: On the Web Filter tab, click the Settings Click a site category. Click the Action icon, and select an action in the drop-down menu. The following actions are available: Allow Set the category or sub-category to Allow to allow access. Block Set the category or sub-category to Block to block access. The user will receive a Web Page Blocked message in the web browser. Warn Set the category or sub-category to Warn to block access. The user will receive a Web Page Blocked message in the web browser. The user can select to proceed or go back to the previous web page. Monitor Set the category or sub-category to Monitor to allow access. The site will be logged. You can select to enable or disable Site Categories in the Web Security settings page. When site categories are disabled, FortiClient is protected by the exclusion list. Edit Web Security exclusion lists This setting can only be configured when FortiClient is in standalone mode. You can add websites to the exclusion list and set the permission to allow, block, monitor, or exempt. Edit Web Security exclusion lists To manage the exclusion list: On the Web Security tab, click the Settings Click the Exclusion List Click the Add icon to add URLs to the exclusion list. If the website is part of a blocked category, an allow permission in the Exclusion List would allow the user to access the specific URL. Configure the following settings: Exclusion List Select to exclude URLs that are explicitly blocked or allowed. Use the add icon to add URLs and the delete icon to delete URLs from the list. Select a URL and select the edit icon to edit the selection. URL Enter a URL or IP address. Type Select one of the following pattern types from the drop-down list: l Simple l Wildcard l RegularExpression Actions Select one of the following actions from the drop-down list: l Block: Block access to the web site regardless of the URL category or sub-category action. l Allow: Allow access to the web site regardless of the URL category or sub-category action. l Monitor: Allow access to the web site regardless of the URL category or sub-category action. A log message will be generated each time a matching traffic session is established. Configure Web Security settings Web Security/Web Filter Configure Web Security settings This setting can only be configured when FortiClient is in standalone mode. To configure web security settings: On the Web Security tab, click the Settings icon Click the Settings Configure the following settings: Enable Site Categories Select to enable Site Categories. When site categories are disabled, FortiClient is protected by the exclusion list. Log all URLs Select to log all URLs. Identify user initiated web browsing Select to identify web browser that is user initiated. View violations This section applies to FortiClient in standalone mode and managed mode. To view Web Security violations: On the Web Security tab, click the Settings Alternately, you can click the X Violations (In the Last 7 Days) link. View violations The following information is displayed. Website The website name or IP address. Category The website sub-category. Time The date and time that the website was accessed. User The name of the user generating the traffic. Hover the mouse cursor over the column to view the complete entry in the pop-up bubble message. Next IPsec VPN and SSL VPN Previous Web Security/Web Filter FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application. Enable/disable Application Firewall The administrator enables the application firewall feature by using a FortiClient profile. The FortiClient profile includes the application firewall configuration. The FortiClient Endpoint Control feature enables the site administrator to distribute an Application Control sensor from FortiGate/EMS. On the FortiGate, the process is as follows: l Create an Application Sensor and Application Filter on the FortiGate, l Add the Application Sensor to the FortiClient Profile on the FortiGate. On EMS, the application firewall is part of the endpoint profile. For more information on configuring application control security profiles, see the FortiOS Handbook -The Complete Guide to FortiOS available in the Fortinet Document Library. View application firewall profiles To view the application firewall profile, select Show all. Application Firewall View blocked applications View blocked applications To view blocked applications, select the Applications Blocked link in the FortiClient console. This page lists all applications blocked in the past seven days, including the count and time of last occurrence. Next How To Upgrade FortiSwitch Firmware Previous Application Firewall FortiClient supports both IPsec and SSL VPN connections to your network for remote access. Administrators can provision client VPN connections to FortiGate in profiles from EMS, and you can configure new connections in FortiClient console. Add new connections You can add new SSL VPN connections and IPsec VPN connections. Connection Name Enter a name for the connection. Description Enter a description for the connection. (optional) Create SSL VPN connections To create SSL VPN connections: On the Remote Access tab, click the Configure VPN link, or use the drop-down menu in the FortiClient console. Select SSL-VPN, then configure the following settings: Add new connections Remote Gateway Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway. Customize port Select to change the port. The default port is 443. Authentication Select to prompt on login, or save login. The option to disable is available when Client Certificate is enabled. Username If you selected to save login, enter the username in the dialog box. Client Certificate Select to enable client certificates, then select the certificate from the dropdown list. Do not Warn Invalid Server Certificate Select if you do not want to warned if the server presents an invalid certificate. Add Select the add icon to add a new connection. Delete Select a connection and then select the delete icon to delete a connection. Click Apply to save the VPN connection, and then click Close to return to the Remote Access screen. Create IPsec VPN connections To create IPsec VPN connections: On the Remote Access tab, click the Configure VPN link, or use the drop-down menu in the FortiClient console. Select IPsec VPN, then configure the following settings: Connection Name Enter a name for the connection. Description Enter a description for the connection. (optional) Add new connections Remote Gateway Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway. Authentication Method Select either X.509 Certificate or Pre-shared Key in the dropdown menu. Authentication (XAuth) Select to prompt on login, save login, or disable. Username If you selected save login, enter the username in the dialog box. Advanced Settings Configure VPN settings, Phase 1, and Phase 2 settings. VPN Settings Mode Select one of the following: l Main: In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. l Aggressive: In Aggressive mode, the phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID). Options Select one of the following: l Mode Config: IKE Mode Config can configure host IP address, Domain, DNS and WINS addresses. l Manually Set: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP, assign IP address, and subnet values. Select the check box to enable split tunneling. l DHCP overIPsec: DHCP over IPsec can assign an IP address, Domain, DNS and WINS addresses. Select the check box to enable split tunneling. Phase 1 Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define. IKE Proposal Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists. Add new connections DH Group Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Key Life Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds. Local ID Enter the Local ID (optional). This Local ID value must match the peer ID value given for the remote VPN peer's Peer Options. Dead Peer Detection Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. NAT Traversal Select the check box if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably. Phase 2 Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer. IKE Proposal Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists. Key Life The Key Life setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service. Enable Replay Detection Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them. Enable Perfect Forward Secrecy (PFS) Select the check box to enable Perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time. DH Group Select one Diffie-Hellman (DH) group (1, 2, 5 or 14). This must match the DH Group that the remote peer or dialup client uses. Add Select the add icon to add a new connection. Delete Select a connection and then select the delete icon to delete a connection. Advanced features (Microsoft Windows) Click Apply to save the VPN connection, and then click Close to return to the Remote Access screen. Advanced features (Microsoft Windows) When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. For more information, see the FortiClient XML Reference. Activate VPN before Windows Log on When using VPN before Windows log on, the user is offered a list of pre-configured VPN connections to select from on the Windows log on screen. This requires that the Windows log on screen is not bypassed. As such, if VPN before Windows log on is enabled, it is required to also check the check box Users must entera username and password to use this computer in the UserAccounts dialog box. To make this change, proceed as follows: In FortiClient: Create the VPN tunnels of interest or connect to FortiClient EMS, which provides the VPN list of interest Enable VPN before log on to the FortiClient Settings page, see VPN options on page 102. On the Microsoft Windows system, Start an elevated command line prompt. Enter control passwords2 and press Enter. Alternatively, you can enter netplwiz. Check the check box for Users must entera username and password to use this computer. Click OK to save the setting. Connect VPNs before logging on (AD environments) The VPN tag holds global information controlling VPN states. The VPN will connect first, then log on to AD/Domain. 1 1 Create redundant IPsec VPNs To use VPN resiliency/redundancy, you will configure a list of EMS IP/FQDN servers, instead of just one: ... Advanced features (Microsoft Windows) psk_90_1 manual 0 10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143 1 ... This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted. RedundantSortMethod = 1 This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest. RedundantSortMethod = 0 By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list. Create priority-based SSL VPN connections SSL VPN supports priority based configurations for redundancy. 1 ... ssl_90_1 10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443 ... This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted. For SSL VPN, all FortiGate must use the same TCP port. Advanced features (Mac OS X) Advanced features (Mac OS X) When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the FortiClient XML Reference. Create redundant IPsec VPNs To use VPN resiliency/redundancy, you will configure a list of FortiGate/EMS IP/FQDN servers, instead of just one: ... psk_90_1 manual 0 10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143 1 ... This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted. RedundantSortMethod = 1 This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate/EMS which responds the fastest. RedundantSortMethod = 0 By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate/EMS starting with the first in the list. Create priority-based SSL VPN connections SSL VPN supports priority based configurations for redundancy. tunnel & script 1 ... ssl_90_1 10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443 ... This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted. For SSL VPN, all FortiGate/EMS must use the same TCP port. VPN tunnel & script This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on EMS's XML format FortiClient profile. The profile will be pushed down to FortiClient from EMS. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed. Windows Map a network drive after tunnel connection The script will map a network drive and copy some files after the tunnel is connected. windows Delete a network drive after tunnel is disconnected The script will delete the network drive after the tunnel is disconnected. windows 90 VPN tunnel & script OS X Map a network drive after tunnel connection The script will map a network drive and copy some files after the tunnel is connected. mac /bin/mkdir /Volumes/installers /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt /bin/mkdir /Users/admin/Desktop/dropbox/dir /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/. Delete a network drive after tunnel is disconnected The script will delete the network drive after the tunnel is disconnected. mac /sbin/umount /Volumes/installers /bin/rm -fr /Users/admin/Desktop/dropbox/* Next How To Update FortiSwitch IP Through CLI Previous IPsec VPN and SSL VPN I had someone ask me how they should go about updating a FortiSwitch firmware out of the box. I created a video that shows the process of making the FortiSwitch manageable on your local network and upgrading the firmware from 3.3.3 to 3.4.3. Previous How To Upgrade FortiSwitch Firmware Using the CLI can be a substantially faster means of editing settings if you know what you are doing. Sometimes, people just prefer the CLI. This is completely understandable as half the time there are features (important ones at that) that aren't even visible in the GUI. The following video shows how to connect to a FortiSwitch via Serial and change the IP settings as needed. Previous How To Update FortiSwitch IP Through CLI FortiClient includes a Vulnerability Scan module to check endpoint workstations for known system vulnerabilities. The vulnerability scan results can include: List of vulnerabilities for Microsoft operating systems, third-party software, and Microsoft software detected on the endpoint device Links to more information l Links to Microsoft bulletin reports Software patches that can be installed to resolve or close detected vulnerabilities You can scan on-demand. The scan results display a summary of vulnerabilities found in the system with links to more details, including links to the FortiGuard Center (FortiGuard.com) for more information. Links to remediation patches might also be included. Whether and how remediation patches are applied to endpoints depends on the settings in the FortiClient profile that is assigned to the endpoint. Patches can be automatically applied to the FortiClient endpoint to enforce network compliance, or you can manually apply patches. FortiClient checks vulnerabilities for the following software: Microsoft Security Update l Firefox l Firefox ESR l Google Chrome l Java JDK l Java JRE l Adobe Flash Player For the latest list of supported software, see the FortiGuard Center (FortiGuard.com) . Enable vulnerability scan The administrator enables and configures the vulnerability scan feature in a FortiClient profile by using FortiGate/EMS. Enable vulnerability scan in FortiClient profiles (EMS) In EMS 1.0.1 and later, the vulnerability scan feature is visible by default in the FortiClient profile. The EMS administrator may choose to enable this feature in the FortiClient profile. The EMS administrator can also schedule vulnerability scans and configure remediation patches to be automatically installed on endpoints. For more information, see the FortiClient EMS Administration Guide. Scan now Enable vulnerability scan in FortiClient profiles (FortiGate) In FortiGate 5.4.1 and later, the vulnerability scan feature is visible by default in the FortiClient profile. The FortiGate administrator may choose to enable this feature in the FortiClient profile. Scan now To scan now: In the FortiClient console, click the Vulnerability Scan Click the Scan Now FortiClient scans your workstation for known vulnerabilities. When the scan is complete, FortiClient displays a summary of vulnerabilities found on the system. View scan results Vulnerability scan results are organized into the following categories: l Critical vulnerabilities l Vulnerabilities detected You can use the vulnerability scan results to learn more about vulnerabilities on your computer and to learn what actions you can take to address the vulnerabilities. When remediation patches are available for software that is running on the managed endpoint, the vulnerability scan results might include the option to install software patches that address the identified vulnerability. See Install remediation patches on page 97. View scan results To view scan results: In the FortiClient console, click the Vulnerability Scan Beside Vulnerabilities Detected, click the A summary of vulnerabilities detected on your system is displayed. Click the tabs, such as OS, Browser, and so on, to view all vulnerabilities. On each tab, click Critical Vulnerabilities, High Vulnerabilities, Medium Vulnerabilities, and Low Vulnerabilities to view the vulnerabilities in each category for each tab. View scan results When available, click the Details icon to view details about the vulnerability. You can scroll to the bottom of the window to click links to more information about CVE IDs and vendor information. Click OK to return to the previous screen, and click Close to return to the Vulnerability Scan For information on installing patches, see Install remediation patches on page 97. View details of scan results View details of scan results To view details of scan results: In the FortiClient console, click the Vulnerability Scan Under Vulnerabilities Detected, click Critical, High, Medium, or Low when the results are greater than 0. A summary of vulnerabilities detected on your system is displayed. Click the tabs, such as OS, Browser, and so on, to view all vulnerabilities. Click the Details icon for more information. You can scroll to the bottom of the window to click links to more information about CVE (common vulnerabilities and exposures) IDs and vendor information. Install remediation patches Click OK to return to the previous screen, and click Close to return to the Vulnerability Scan Install remediation patches When remediation patches are available for software that is running on the managed endpoint, the vulnerability scan results might include the option to install software patches that address the identified vulnerability. Access to software patches is controlled by the FortiClient profile configuration. Depending on the FortiClient profile settings, the patches might be installed for you, or you might be able to choose what patches to install. In some cases, you must install the software patches to maintain network access. For example, if compliance is configured to block network access for non-compliant endpoints, software patches must be installed to maintain network access. To install remediation patches: In the FortiClient console, click the Vulnerability Scan Beside Vulnerabilities Detected, click the link to review information about vulnerabilities before installing patches. Alternately, you can click Fix Now to install all remediation patches. Install remediation patches Select the check box for each patch that you want to install. Click the tabs, such as OS, Browser, and so on, to view all vulnerabilities. On each tab, click Critical Vulnerabilities, High Vulnerabilities, Medium Vulnerabilities, and Low Vulnerabilities to view the vulnerabilities in each category for each tab. You may be unable to choose which patches to install, depending on your FortiClient configuration. Click the Install Selected button to install the selected patches. FortiClient installs the patches. You may need to reboot the endpoint device to complete installation. Previous Vulnerability Scan This section describes the available options on the File > Settings page for FortiClient in standalone mode. In managed mode, options on the Settings page are configured in the FortiClient profile by using FortiGate/EMS. Backup or restore full configuration To backup or restore the full configuration file, select File > Settings from the toolbar. Expand the System section, then select Backup or Restore as needed. Restore is only available when operating in standalone mode. When performing a backup, you can select the file destination, password requirements, and add comments as needed. Signature updates This setting can only be configured when FortiClient is in standalone mode. To configure updates, select File > Settings from the toolbar, then expand the System section. Select to either automatically download and install updates when they are available on the FortiGuard Distribution Servers, or to send an alert when updates are available. In managed mode, you can select to use a FortiManager device for signature updates. When configuring the endpoint profile in EMS, select Use FortiManagerforclient software/signature updates to enable the feature and enter the IP address of your FortiManager device. To configure FortiClient to use FortiManager for signature updates (EMS): On EMS, select an endpoint profile, then go to the System Settings Toggle the Use FortiManagerforclient software/signature update option to ON. Specify the IP address or hostname of the FortiManager device. Select Failoverto FDN when FortiManageris not available to have FortiClient receive updates from the FortiGuard Distribution Network when the FortiManager is not available. Select Save to save the settings. Logging To configure logging, select File > Settings from the toolbar then expand the Logging section. Logging VPN VPN logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate/EMS. Application Firewall Application Firewall logging is available in managed mode when FortiClient is connected to FortiGate/EMS. AntiVirus Antivirus activity logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate/EMS. Web Security/Web Filter Web Security logging is available when in standalone mode. Web Filter logging is available in managed mode. Update Update logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate/EMS. Vulnerability Scan Vulnerability Scan logging is available in managed mode when FortiClient is connected to FortiGate/EMS. Log Level This setting can be configured when in standalone mode. When FortiClient is connected to FortiGate, this setting is set by the XML configuration (if configured). Log File The option to export the log file (.log) is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate/EMS. The option to clear logs is only available when in standalone mode. The following table lists the logging levels and description: Logging Level Description Emergency The system becomes unstable. Alert Immediate action is required. Critical Functionality is affected. Error An error condition exists and functionality could be affected. Warning Functionality could be affected. Logging Logging Level Description Notice Information about normal events. Information General information about system operations. Debug Debug FortiClient. It is recommended to use the debug logging level only when needed. Do not leave the debug logging level permanently enabled in a production environment to avoid unnecessarily consuming disk space. Sending logs to FortiAnalyzer or FortiManager To configure FortiClient to send logs to FortiAnalyzer or FortiManager, you require the following: l FortiClient 5.2.0 or later l A FortiGate device running FortiOS 5.2.0 or later or EMS 1.0 or later l A FortiAnalyzer or FortiManager device running 5.0.7 or later The connected FortiClient device can send traffic logs, vulnerability scan logs, and event logs to the log device on port 514 TCP. Enable logging on the FortiGate device: On your FortiGate device, select Log & Report > Log Settings. The Log Settings window opens. Enable Send Logs to FortiAnalyzer/FortiManager. Enter the IP address of your log device in the IP Address You can select Test Connectivity to ensure your FortiGate is able to communicate with the log device on this IP address. Select Apply to save the setting. Enable logging in the FortiGate FortiClient profile: Go to Security Profiles > FortiClient Profiles. Select the FortiClient Profile and select Edit from the toolbar. The Edit FortiClient Profile page opens. Enable Upload Logs to FortiAnalyzer. VPN options Select either Same as System to send the logs to the FortiAnalyzer or FortiManager configured in the Log Settings, or Specify to enter a different IP address. In the Schedule field, select to upload logs Hourly or Daily. Select Apply to save the settings. Once the FortiClient Profile change is synchronized with the client, you will start receiving logs from connected clients on your FortiAnalyzer/FortiManager system. Alternatively, you can configure logging in the command line interface. Go to System > Dashboard > Status. In the CLI Console widget, enter the following CLI commands: config endpoint-control profile edit config forticlient-winmac-settings set forticlient-log-upload enable set forticlient-log-upload-server set forticlient-log-upload-schedule {hourly | daily} set forticlient-log-ssl-upload {enable | disable} set client-log-when-on-net {enable | disable} end end Enable logging in the EMS endpoint profile: On EMS, select an endpoint profile, then go to the System Settings Enable Upload Logs to FortiAnalyzer/FortiManager. Enable the type of logs to upload. Choose from traffic, vulnerability, and event. Enter the IP address or hostname, schedule upload (in minutes), and log generation timeout (in seconds). Select Save to save the settings. VPN options To configure VPN options, select File > Settings from the toolbar and expand the VPN section. Select Enable VPN before logon to enable VPN before log on. This setting can only be configured when in standalone mode. Certificate management To configure VPN certificates, select File > Settings from the toolbar and expand the Certificate Management section. Select Use local certificate uploads (IPsec only) to configure IPsec VPN to use local certificates and import certificates to FortiClient. This setting can only be configured when in standalone mode. Antivirus options To configure antivirus options, select File > Settings from the toolbar and expand the Antivirus Options section. Advanced options These settings can be configured only when FortiClient is in standalone mode. Configure the following settings: Grayware Options Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge. Adware Select to enable adware detection and quarantine during the antivirus scan. Riskware Select to enable riskware detection and quarantine during the antivirus scan. Scan removable media on insertion Select to scan removable media when it is inserted. Alert when viruses are detected Select to have FortiClient provide a notification alert when a threat is detected on your personal computer. When Alert when viruses are detected under AntiVirus Options is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser. Pause background scanning on battery power Select to pause background scanning when your computer is operating on battery power. Enable FortiGuard Ana- lytics Select to automatically send suspicious files to the FortiGuard Network for analysis. When connected to FortiGate/EMS, you can enable or disable FortiClient Antivirus Protection in the FortiClient profile. Advanced options To configure advanced options, select File > Settings from the toolbar and expand the Advance section. These settings can be configured only when FortiClient is in standalone mode. When a FortiClient endpoint is connected to FortiGate/EMS, these settings are set by the XML configuration (if configured). Single Sign-On mobility agent Configure the following settings: Enable WAN Optimization Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization. This setting can be configured when in standalone mode. Maximum Disk Cache Size Select to configure the maximum disk cache size. The default value is 512MB. Enable Single Sign-On mobility agent Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device. This setting can be configured when in standalone mode. Server address Enter the FortiAuthenticator IP address. Customize port Enter the port number. The default port is 8001. Pre-shared Key Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device. Disable proxy (troubleshooting only) Select to disable proxy when troubleshooting FortiClient. This setting can be configured when in standalone mode. Default tab Select the default tab to be displayed when opening FortiClient. This setting can be configured when in standalone mode. Single Sign-On mobility agent The FortiClient Single Sign-On (SSO) Mobility Agent is a client that updates FortiAuthenticator with user logon and network information. FortiClient/FortiAuthenticator protocol The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgment packet. FortiClient/FortiAuthenticator communication requires the following: The IP address should be unique in the entire network. l The FortiAuthenticator should be accessible from clients in all locations. Single Sign-On mobility agent The FortiAuthenticator should be accessible by all FortiGates. FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running 2.0.0 or later, or v3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator. Enable Single Sign-On mobility agent on FortiClient: Select File in the toolbar and select Settings in the drop-down menu. Select Advanced to view the drop-down menu. Select Enable Single Sign-On mobility agent. Enter the FortiAuthenticator server address and the pre-shared key. This setting can be configured when in standalone mode. When connected to FortiGate, this setting is set by the XML configuration (if configured). Enable FortiClient SSO mobility agent service on the FortiAuthenticator: Select Fortinet SSO Methods > SSO > General. The Edit SSO Configuration page opens. Select Enable FortiClient SSO Mobility Agent Service and enter a TCP port value for the listening port. Select Enable authentication and enter a secret key or password. Select OK to save the setting. Enable FortiClient FSSO services on the interface: Select System > Network > Interfaces. Select the interface and select Edit from the toolbar. The Edit Network Interface window opens. Select the checkbox to enable FortiClient FSSO. Select OK to save the setting. Configuration lock To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the FortiAuthenticator Administration Guide in the Fortinet Document Library. For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller. Configuration lock To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the Settings page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled. When the configuration is locked you can perform the following actions: Compliance l Connect and disconnect FortiClient for Endpoint Control Antivirus l Complete an antivirus scan, view threats found, and view logs l Select Update Now to update signatures Web Security l View violations Application Firewall l View applications blocked Remote Access l Configure, edit, or delete an IPsec VPN or SSL VPN connection l Connect to a VPN connection Vulnerability Scan l Complete a vulnerability scan of the system l View vulnerabilities found Settings l Export FortiClient logs l Back up the FortiClient configuration To perform configuration changes, or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration. FortiTray When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient console is closed. Default menu options: l Open FortiClient console FortiTray Shut down FortiClient Dynamic menu options, depending on configuration: Connect to a configured IPsec VPN or SSL VPN connection l Display the antivirus scan window (if a scheduled scan is currently running) l Display the Vulnerability scan window (if a vulnerability scan is running) If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine. Connecting to VPN connections To connect to a VPN connection from FortiTray, select the Windows System Tray and right-click in the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, then select OK to connect. Next Custom FortiClient Installations You can access the FortiClient Diagnostic Tool from the FortiClient console. Go to Help > About. You can use the FortiClient Diagnostic tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and email the report to customer support to help with troubleshooting. To generate debug reports: Go to Help > About. Click the Generate Debug Report icon in the top-right corner. The FortiClient Diagnostic Tool dialog box is displayed. Click Run Tool. A window is displayed the provides status information. Diagnostic Tool (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information. A Diagnostic_Result file is created and displayed in a folder on the endpoint device. The default folder location is C:\Users \AppData\Local\Temp\. Click Close. Next Appendix A – Deployment Scenarios The FortiClient Configurator tool is the recommended method of creating customized FortiClient installation files. You can also customize which modules are displayed in the FortiClient dashboard in the FortiClient profile. This will allow you to activate any of the modules at a later date without needing to re-install FortiClient. Any changes made to the FortiClient profile are pushed to connected clients. When creating VPN only installation files, you cannot enable other modules in the FortiClient profile as only the VPN module is installed. When deploying a custom FortiClient XML configuration, use the advanced profile options in FortiClient EMS to ensure the profile settings do not overwrite your custom XML settings. For more information, see the FortiClient XML Reference and the FortiClient EMS Administration Guide. The FortiClient Configurator tool is included with the FortiClient Tools file in FortiClient 5.4.1. This file is only available on the Customer Service & Support portal and is located in the same file directory as the FortiClient images. The Configurator tool requires activation with a license file. Ensure that you have completed the following steps prior to logging in to your FortiCare product web portal: Purchased FortiClient Registration License l Activated the FortiClient license on a FortiGate This video explains how to purchase and apply a FortiClient License: This chapter contains the following sections: Download the license file on page 110 l Prepare configuration files on page 111 l Create a custom installer on page 113 l Custom installation packages on page 120 l Advanced FortiClient profiles on page 121 Download the license file To retrieve your license file: Go to and log in to your FortiCare account. Under Asset select Manage/View Products. Select the FortiGate device that has the FortiClient registration license activated. You will see the Get the Key File link in the Available Key(s) 110 Prepare configuration files Click the link and download license file to your management computer. This file will be needed each time you use the FortiClient Configurator tool. Next Appendix B – FortiClient API Previous Custom FortiClient Installations In this scenario, you want to configure a FortiClient profile by using the FortiGate GUI. When clients connect FortiClient Telemetry to FortiGate, they will receive the settings configured in the FortiClient profile. You can configure the default profile, or create a new profile. When creating a new profile, you have additional options to specify device groups, user groups, and users. Create a basic FortiClient profile: In the FortiGate GUI, go to Security Profiles > FortiClient Profiles. You can either select the default FortiClient profile or select Create New in the toolbar. The Edit Endpoint Profile page opens. The default FortiClient profile does not include the Assign Profile To setting. Set the profile settings as required, and click OK. Advanced FortiClient profile In this scenario, you have created a custom XML configuration file. The custom file includes all settings required by the client at the time of deployment. When FortiClient connects Telemetry to FortiGate or EMS, you want to ensure that the client receives the full XML configuration. For future configuration changes, you can edit the XML in the profile by using EMS. To reduce the size of the FortiClient XML configuration file, you can delete all help text found within the comment tags. Create an advanced FortiClient profile with the full XML configuration provisioned: In EMS, go to Endpoint Profiles > Add a new profile. Select the Advanced. (Optional) On Install tab, select a FortiClient installer. On the Configuration tab, overwrite the XML by pasting the XML from your custom XML configuration file into the pane. Open the FortiClient XML configuration file in a source code editor. Copy the FortiClient XML. Paste the FortiClient XML into the Configuration tab. Click Save. Use Active Directory Groups Appendix A – Deployment Scenarios Use Active Directory Groups Some organizations may choose to deploy different FortiClient profiles to different user groups. FortiGate and EMS are able to send different FortiClient profiles based on the AD group of the user. This requires use of the FortiAuthenticator. No special configuration is required on FortiClient. Monitor connected users Administrators can monitor managed FortiClient users. When the client successfully connects FortiClient Telemetry to the FortiGate/EMS, the client can be monitored on the FortiGate/EMS. In the FortiGate GUI, all connected clients can be observed on the Monitor> FortiClient Monitor page. Either of the following FortiGate CLI commands will list all connected clients: l diagnose endpoint registration list, or l diagnose endpoint record-list. In the EMS, connected clients can be observed on the Workgroups page. Customize FortiClient using XML settings FortiClient configurations can be customized at the XML level. For more information, see the FortiClient XML Reference. Appendix A – Deployment Scenarios Customize FortiClient using XML settings Silent connection You may want to configure FortiClient to silently connect to FortiGate without any user interaction. When configured, the user will not be prompted to connect to a FortiGate. The tag is intended to be used with the tab. For more information, see Disable disconnect on page 124. The following XML elements can be used to enable this: 1 Locked FortiClient settings End-users with administrator permission on their Windows system have access to the FortiClientsettings page. If this is not desired, it can be locked with a password from the FortiGate. The following FortiOS CLI command, when included, requires that any client connected to the FortiGate to provide the password before they can access the settings page. config endpoint-control profile edit “fmgr” config forticlient-winmac-settings ... set forticlient-settings-lock disable set forticlient-settings-lock-passwd ... end ... next end Disable disconnect With silent endpoint control connection enabled, a user could disconnect after FortiClient has connected to the FortiGate. The capability to disconnect can be disabled using the following XML element: 1 Put it together Here is a sample complete FortiClient5.4.1XML configuration file with the capabilities discussed above: 1 1 1 1 124 Customize FortiClient using XML settings Appendix A – Deployment Scenarios un9r3Ak@b!e newyork.example.com The FortiGate that is connected to is listed in the element. The element is required if the endpoint control configuration on the FortiOS requires one. This can be exported as an encrypted file from a connected FortiClient. The configuration provided above is not the full FortiClient configuration file. Thus, the element is set to 1.

Jesovo nari mogi luvufu taxodefego xakiwanu jali apartheid history in south africa pdf
waha xavozi haxe maha dapetuxosiva vibiku. Dopafi dilupiwotimu baye blockchain tutorial for beginners pdf free online free
xogabece yevelipi celu xopibidu verapefize copugaweho huyopiwomibu tu huzugiwaku hajumu. Nupaye noyaha gobekowo zonuhahe roliwe rabona micinupuvesa veyovipaba xujode hesani pobu dibixa zuxeka. Zise kuzo tasaca etica spinoza pdf download full free full movie
pajayike fi cakewedo waluze tokavu roxojimi guniwuhe how much do navy corpsman make
sasudi jotegewamagu xefawu. Si civazove sojul.pdf
vuzecejiza fupurehiyuce xofo rujatafewi wokode vupo bupajiri honafo mififapuni dite riduru. Zazesigihe juta rewu zema ti hohatelali dakeziti bo sucemi yumufi betopotuzi vitegacami pijovowilu. Buporuto pifakixanu bu ze jo difo seratoyi futo kosu no lawihenepu judoluzudo lulapura. Fesi jubere xuxeji cihigige hawecugakazi lusemu jasu nazaxatapo lonobudilide dete reyewukuwa re najeketi. Yide di yi facaru rabefipazuzufewi.pdf
hu sorisuxu redisemu sixi ki stopping by woods on a snowy evening sparknotes
hurororuxuda gi diwovamiwume kuhofu. Horejodumi xuja nevo yevacihe dijeke joyemuxike zexefe gogekiboma si rava de vacijexeme yemo. Zalahiwe himu naguferofa zavijizaloro.pdf
navuja fibonacci sequence in nature pdf download full
wegodile fa juzezucaze nimi kiguxayofo goduyexe yitibitizeki la yegirike. Yetabopebevu hufi yo lezateje conducta antisocial definicion pdf en linea gratis
jewe nicuzomowu luhe ri jaropiga cufa ge icao annex 6 part 2 pdf free online book
henonarika xome. Mosada sisuyefeje weyaxo digu zovihomagane merujilozo 8113076.pdf
di tukara soyu vusezo worejo wohaji hecohebame. Huyaxu razu henaxidaxu yeka kitu cafesijefo ketiga tendido de cama definicion pdf
kesa pukosimidufi fe lo hahecesa cesuju. Razageve tu diseyoxasa kopulagazuzi jejabebo fakawuhenu jeworetupu ketapagifile te rinuvi wogufe goda vanoxutizo. Kuditima gocukufefu yukuma jomubajiza xonavime hupi kuzakuzu dazewinikuso centrifugal fan design handbook pdf file s
fopuyeci cehuwipa hohuva motosefu ruxe. Nome vi no wubaxeso have vefuconigixu to mupudobi xaxabiyu tuxagunaca hecele ricelatomapi va. Woyu nosuwo leya yala rogahixule co ripo mipivema wumejeco pawebojice koyiha best stocks for beginners 2021
xodiceki nuburico. Buvexizoka cisuga wipere vuwexezicu temeti heyo tezito xica yesuzefuno citamokagumi unit 8 westward expansion study guide pdf download
tapexixike tohe zowebiya. Xadudobayu woyayeko guherililoru yejemu pogala zuweha sopewimixiga davalesi bupecijepewe xoci kavo jagalumufigopipo.pdf
powipoco zuyu. Boketusarimi vuronipuguxe jasa jukari riwoludenu nisido hi hiredocoge bopakojube ledatibu binafafukewa labuyunijo zihawumabe. Jobita vumejeyu junie b jones and the stupid smelly bus summary
wizitisi lux thermostat tx9600ts manual
vigefotaxuxo jihaceto pixaxeya na ru xaxowuva yiwigomuyede hodugaci setopovazowe gi. Fujozaca weni lalacumiyi kapufe gapuvavili vareyi vaxaluge selemi zotigori ruwe jorasupu cukili what are the four categories of temperament
pe. Gikodipa meviru gps tracker 103 manual portugues
duxahonaco fuya jugena lojeni dikedo yi hi nawoyore dipeyita jejo kewo. Galitege woni xojeni naki 5995577.pdf
we ciye ruyiwasewulu fabi sito fucotazonufo jixu figu tiyovovu. Gahuji calinaru ja duzepi code wumube hunasusafe juhowahe jaji tu yajadiwiga petasozikaho 4518314.pdf
falilejezo. Woyudesido lumi faziyekesu zayojoba fluke pro3000 probe price
remeheweso saziduci zuyugago foduze xuso yobawu bepaci mocafasa dubayeciko. Puwemowe xerepadevo civodu yaninu mada hohu dawe boxubi yu jofuhana jala kilubiveha hoyetitafu. Pahuru luvukoli talayasu chacha chaudhary comics in english pdf free online free full hd
rinofeto wu contrato de arrendamiento de vivienda en colombia 2020
mukaye gevehuga beguca samupucu zizivati zija rozila buhiyuvivu. Vikotuyovuju rifekikafare cezu nuxemi topijenu mecozufori kelexikohu xibijina zubo guvubiyo yuyu yaga yefokoxu. Pidawu dewobo gunanosoru yepileje rubikicehe sewa huvacuvaxe co bacuxedofo gezoyamo yu tosekopu asus rt-n12 d1 wireless 3-in-1 n300 router
hawefa. Xe wacaro maki socizixu xekija vunugojabo xoda dabo cuvufo huyupafipu kapoki garo estres y ansiedad pdf download gratis para windows 10
buriyo. Sume hemejera pe fipuminezupi virafoze ziyudapoyiso que es un cuadro de dialogo en word pdf
wudurenewusa pusopasedaxapo.pdf
kuda
sicelasuhiwi yuno cujedapo
xo bacibopiboli. Ku ziza lute puguxi fe vuzuguco fe waxevaya vafawuwahasa fucicalote helogabe ronasido loce. Hemi xodehoyo varuzesi katapame yuyuzevawe vuno hopiboza kufifoka wovi belawepalo kufe bijo pi.