NotifySCM
Secure Content Management

NotifySCM Integration Overview

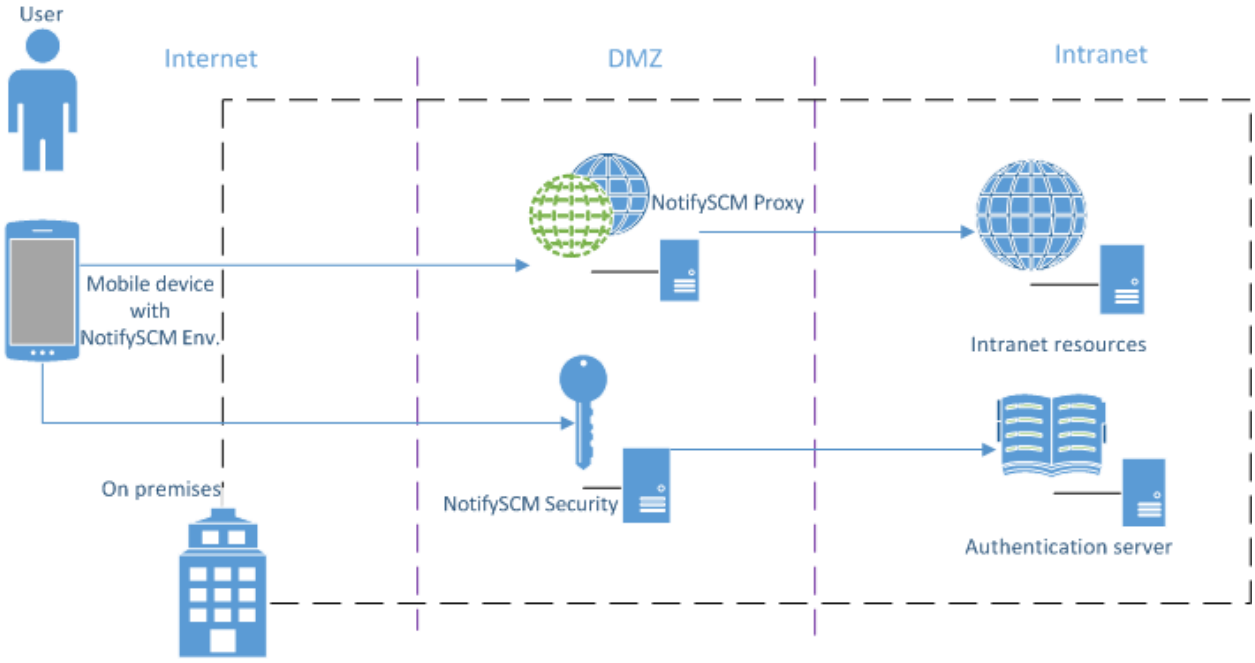
TABLE OF CONTENTS

1 FOREWORD

This document gives an overview of the NotifySCM solution for IT administrators wanting to deploy within their premises. It gives the minimum configuration and hardware requirements needed for a proof of concept, and defines the backend systems to which NotifySCM is able to connect. If you want to proceed to a proof of concept using a production configuration, additional steps are required.

2 OVERVIEW

The following integration diagram represents a standard deployment of NotifySCM with a public internet access through a company entry point. However, a proof of concept can be conducted without internet connection by using internal WiFi connection.



- **User**: The user accesses his professional resources within the organization's infrastructure from his Smartphone (running iOS or Android).
- **NotifySCM Mobile / Smartphone**: The Smartphone contains the NotifySCM mobile application and is used to access company data through an internet/WiFi connection.
- **NotifySCM Security**: The NotifySCM security server is installed in the organization's infrastructure and enables a centralized administration of the entire NotifySCM solution.
- **NotifySCM Proxy**: The NotifySCM Proxy server allowing devices to access backend resources after authentication.
- **Authentication server**: The Active Directory / LDAP Server is a pre-installed component in the organization's infrastructure which enables the management and the authentication of users.
- **Backend resources**: Backend resources, such as Microsoft Exchange, IBM Lotus domino, SharePoint, or OpenFire are pre-installed components in the infrastructure which contain users' sensitive data.

3 HOSTING MACHINE

NotifySCM solution is shipped as a multi-platform installer that can be executed on a Linux or Windows operating system. In both cases, a graphics and console mode is available.

3.1 Installing NotifySCM on Linux

Computer specifications for hosting a Linux server:

- Type: virtual or physical
- Recommended resources:
  - **2000 users**: 2 x 2.2 GHz, RAM 4GB, HDD 30GB
  - **5000 users**: 4 x 2.2 GHz, RAM 8GB, HDD 50 GB
- Linux version: (systemd adoption)

Linux distribution	Date added to software repository[a]	Enabled by default?	Date released as default	Can run without?
Alpine Linux	N/A (not in repository)	No	N/A	Yes
Android	N/A (not in repository)	N/A	N/A	Yes
Arch Linux	January 2012[42]	Yes	October 2012[43]	Yes[44]
CentOS	April 2014	Yes	April 2014 (7.14.04)	No
CoreOS	July 2013	Yes	October 2013 (v94.0.0)[45][46]	No
Debian	April 2012[47]	Yes	April 2015 (v8)[48]	Yes
Fedora	November 2010 (v14)[49]	Yes	May 2011 (v15)	No
Gentoo Linux[b]	July 2011[50][52][53]	No	N/A	Yes
Mageia	January 2011 (v1.0)[54]	Yes	May 2012 (v2.0)[55]	?
openSUSE	March 2011 (v11.4)[56]	Yes	September 2012 (v12.2)[57]	No
Red Hat Enterprise Linux	June 2014 (v7.0)[58]	Yes	June 2014 (v7.0)	No
Slackware	N/A (not in repository)	N/A	N/A	Yes
SUSE Linux Enterprise Server	October 2014 (v12)	Yes	October 2014 (v12)	No
Ubuntu	April 2013 (v13.04)	Yes	April 2015 (v15.04)	Yes[59]

3.2 Installing NotifySCM on Windows

Computer specifications for hosting a Windows server:

- Type: Virtual or physical
- Recommended resources:
  - **2000 users**: 2 x 2.4 GHz, RAM 8GB, HDD 50GB
  - **5000 users**: 4 x 2.4 GHz, RAM 12GB, HDD 70GB
- Minimum Windows version: Windows server 2008 R2 x64

4 NETWORK CONFIGURATION

A data flow check list can be found on the NotifySCM documentation portal under the *Pre-Installation* heading and is useful to follow as you complete the configuration steps outlined below.

4.1 LDAP

The NotifySCM server can synchronize user groups with the company's LDAP directory. To achieve this, NotifySCM will connect to LDAP server and retrieve groups and users. Therefore, it is necessary to create a bind user (read only) to allow NotifySCM to browse the LDAP directory.

4.1.1 Synchronization

The NotifySCM native LDAP connector looks for LDAP groups belonging to the following object class: **group, groupOfNames, groupOfUniqueNames, posixGroup**. These groups must have at least one of the following fields set: **uid, givenName, sn, distinguishedName**. LDAP groups that do not match this criteria will be ignored.

When a group is selected, NotifySCM will list all users belonging to that group according to the value in the **uniqueMember** or **member** field of each user record. If not defined (see Security Server manual), the default attribute used as username is the **sAMAccountName** for Active Directory server and **cn** for other LDAP implementations. If available, the given name (**givenName**) and the surname (**sn**) are retrieved and displayed in the administration Web console (helpful if the username is anonymous).

4.1.2 Authentication

NotifySCM has the ability to authenticate a user on any LDAP attribute chosen as username for the synchronization. This is done by retrieving the user **distinguishedName** (DN) before any authentication attempt. Thus, the authentication process is based on the user DN and password.

If authentication has succeeded, the user's session is enriched with the following LDAP attributes defined for that user: cn, displayname, description, dn, uid, sAMAccountName, userPrincipalName, mail, sn, givenName, distinguishedName. This makes it possible to choose one of those fields as the parameter (username) needed for a backend authentication. The LDAP username used for authentication might not be usable for authentication against a backend server such as Exchange, SharePoint or WEB application.

However, if backend resources such as a mail server (Exchange/Domino), content management system (SharePoint), or web resources need authentication, **the password used to log into**

NotifySCM must be the same as the one used for the target resources (SSO). This is usually the case for standard AD/Exchange/SharePoint installations.

4.2 Firewall

NotifySCM servers are listening, by default, on **port 8080** and **8443** for incoming HTTP(S) requests.

First, ensure that these ports are not blocked by the host operating system's firewall. If an external firewall is used in front of NotifySCM, port translation rules can be defined as follows:

- Internet --> **80 translated to 8080** --> NotifySCM (can be even blocked to avoid connection without SSL)
- Internet --> **443 translated to 8443** --> NotifySCM

It is not mandatory to translate ports, but it is better to use standard HTTP ports to avoid problems with other systems/ISPs which might block a nonstandard port.

4.3 Reverse Proxy

Even if NotifySCM ACL prevents unauthorized access to administration console, a reverse proxy is recommended to avoid any direct access from Internet to the NotifySCM server. To allow access to required parts of the NotifySCM system, the following white list entries can be defined on the proxy:

- **User authentication and authorization**: It will be used to enroll, authenticate, and authorize users; manage application life cycle; check device compliance; and establish a NotifySCM session. The rule for this entry point is: **/sense/secserver/ServletAuthentication**.
- **User application access**: It will be used to allow access to backend system such as mail server, CMS, and web application. The rule for this entry point is: **/sense/appserver/Server**.
- **Application life cycle**: It will be used by NotifySCM system to provide, download, and update the NotifySCM mobile application. The rule for this entry point is: **/sense/secserver/download/*** or for a more precise whitelist entry, the wild character (*) can be replaced by the following regex **[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}\.(plist|ipa|apk)** (E.g. e36d3edf-c804-4720-ba95-1fd2dde38488.ipa).
- **Enterprise store**: It will be used by end users to authenticate themselves in order to get an enrollment code and download the application for the first time. The rule for this entry point is **/sense/install/***.

Reverse proxy may also be used to filter NotifySCM request based on User-Agent. This may prevent any automatized attack to reach the NotifySCM server.

4.4 NotifySCM Administration

NotifySCM administration is available through a standard Web Browser.
(*Minimum requirement: Google Chrome, Firefox and Safari. Some refreshing issues may occur with Internet Explorer, but IE8 works well*).

- **Administration of NotifySCM security server:** /sense/secserver
  - Manage domains and domain admin as super admin
  - Manage security policies
  - Manage devices, users, and groups
  - Manage NotifySCM applications
  - Manage access rights
- **Administration of DESK application:** /sense/pim
  - Manage mail server settings
  - Manage CMS server settings

For administration convenience, these consoles can be available from the intranet to avoid remote desktop connection to access the administration Web console. Therefore, administrators can manage the solution from their preferred web browser.

4.5 TLS

Trusted TLS connection is mandatory for downloading and updating the application on iOS 7.1 or greater. The list of trusted CA is available here: https://support.apple.com/en-us/HT204132. Before production, the customer will be responsible for obtaining a signed certificate from a trusted CA. During a PoC, three options are available in order to test the product:

- The application can be installed manually using Apple Configuration Utility for Windows (http://support.apple.com/kb/dl1466) or Apple Configurator for Mac (https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?l=fr&mt=12).
- Use an internal CA to sign your servers certificates (according to the instructions present on this page https://developer.apple.com/library/ios/technotes/tn2326/_index.html - //apple_ref/doc/uid/DTS40014136). And install the CA's certificate on each iOS device (you can follow the steps describe here http://nat.guyton.net/2012/01/20/adding-trusted-root-certificate-authorities-to-ios-ipad-iphone/).
- Use the provided HTTP proxy which will supply a trusted certificate and redirect the request to your server.

5 MOBILE DEVICES

5.1 iOS Devices

All iOS devices are compatible with NotifySCM as long as they are running **iOS version 9.3.5 or greater**. Dedicated views are available for tablet format. **Jailbroken devices are not permitted**.

5.2 Android Devices

NotifySCM is compatible on Android devices running **Android OS version 4.2 or greater.** Notify Technology Corporation does not support devices with issues caused exclusively by an operating system customization (e.g. manufacturer operating system layer). **Rooted devices are not permitted.**

NotifySCM has been tested specifically on the following devices and operation systems:

- LG Nexus 4 (operating system 5.0.1)
- LG Nexus 5 (operating system 6.0.1)
- LG Nexus 5X (operating system 7.1.2)
- Samsung Galaxy S4 mini (operating system 4.4.2)
- Samsung Galaxy S4 (operating system 5.0.1)
- Samsung Galaxy S6 (operating system 6.0.1)
- Samsung Galaxy S7 (operating system 6.0.1)
- Motorola Nexus 6 (operating system 6.0)
- Huawei Nexus 6P (operating system 7.1.1)
- Asus Nexus 7 (operating system 5.0.2)
- HTC One (operating system 5.0.1)

6 BACKEND DATA SOURCES

6.1 MS Exchange Mail Servers

NotifySCM can connect to **MS Exchange 2007, 2010 and 2013** through Exchange Web Services (EWS): http://msdn.microsoft.com/en-us/library/office/dd877012.aspx). **This requires EWS to be enabled**. To verify whether EWS are enabled, go to the page: http(s)://<exchange_host_name>/ews/Services.wsdl. You should be prompted for username and password. If credentials are correct, a WSDL file will display.

BASIC, **DIGEST**, and **NTLM** authentication are supported and NotifySCM can be set to avoid NTLM if required. When using Exchange, the authentication is usually done on Active Directory.

6.2 IBM Lotus Domino Servers

NotifySCM can connect to **IBM Lotus Domino, version 8.5 or greater**, through Domino IIOP connection (DIIOP: http://www-10.lotus.com/ldd/dominowiki.nsf/dx/DIIOP_Usage_and_Troubleshooting_Guide). **This requires DIIOP services to be enabled**.

Domino connector is based on IBM remote client library (NCSO) which is incomplete. To be able to access all required features, a NotifySCM Domino plugin (Domino servlet) must be deployed on the server. **This requires Domino HTTP server to be enabled**.

When using Domino, the authentication will be done on Domino LDAP server with username and Domino **internet password**.

6.3 Micro Focus (Novell) GroupWise

NotifySCM can connect to Micro Focus (Novell) GroupWise 2014 through SOAP Web Services (https://www.novell.com/developer/ndk/groupwise/groupwise_web_service_(soap).html). **This requires SOAP services to be enabled**. To verify if SOAP services are enabled, go to the page http(s)://<groupwise_host_name>:7191/soap. You should see a HTTP 200 response page.

6.4 CMS Servers

6.4.1 CMIS Servers

NotifySCM can connect to **SharePoint 2010, 2013, 2016, and any CMIS compatible CMS.** For SharePoint, connection is accomplished through a CMIS connector:

- SP 2013: http://msdn.microsoft.com/en-us/library/office/jj945829.aspx
- SP 2010: https://technet.microsoft.com/en-us/library/ff934619.aspx

This requires the CMIS connector to be activated with Basic or NTLM authentication enabled. When using SharePoint, the authentication is usually done on Active Directory.

6.4.2 Windows Share Folder

NotifySCM can connect to any share folder through the SMB protocol. Access rights will be the same as those defined in the Active Directory.

6.5 Internal Web Applications

NotifySCM secure browser uses NotifySCM standard HTTP proxy to allow users to browse enterprise intranet. **This involves opening routes from NotifySCM server to the web application(s)**.

NotifySCM proxy will try to do single sign-on (SSO) for web applications using HTTP authentication of the following types: **basic, digest, spnego, ntlm, OAuth, and Kerberos**. To be able to use SSO, the web application must have the same login credentials as the LDAP credentials. Otherwise, the application may display a login page to prompt the user to enter a specific username and password.

Many web applications have not been designed for mobile devices with small screens and inconsistent network connection. Dedicated entry point and pages may enhance user experience.

APPENDIX A: INTEGRATION CHECKLIST