Netop Remote Control multi-factor authentication using Radius

Article Number: 370 | Last Updated: Wed, Mar 27, 2019 7:09 AM

Starting with Netop Remote Control version 11.0, the Netop Security Server has been extended to offer authentication against RADIUS (Remote Authentication Dial In User Service) environments. In this version, multi-factor authentication using automatically generated passcodes (e.g. from hardware or software tokens) was supported. Netop Remote Control version 11.6 provides higher security by extending the existing integration with RADIUS. The integration now works also with on-demand generated passcodes, e.g. sent to mobile devices through SMS, or sent via e-mail. The RADIUS authentication flow is as follows: The LDAP credentials are sent to the LDAP server for authentication.Â If successfully authenticated, the LDAP credentials are sent to RADIUS in an Access-Request. RADIUS replies with either an Access-Accept (if the user is not configured to require token authentication), an Access-Reject (containing also the reason for reject), or an Access-Challenge.Â If an Access-Challenge is received, the username and passcode are sent to RADIUS in a new Access-Request. An Access-Accept or Access-Reject is received after RADIUS validates the passcode. In version 12.71, a new Radius authentication flow is supported, where the Radius authentication is done directly with the username and token passcode, instead of expecting a challenge before sending the passcode. When using RADIUS, the Guest's access to the Host is validated based on two factors: Â Â Something the user knows (credentials) Â Â Something the user has (passcode generated by token or received by phone or E-mail). Version 12.76 comes with a new flow, which involves the ability for the RADIUS server to authorize the user via a 2nd factor authentication, independently from the authentication flow implemented by the Netop Security Server. This is achieved by triggering the 2nd factor authentication through additional channels such as push notifications and once the authorization is granted, inform the Netop Security Server of the outcome. This flow needs both the Netop Host and the Netop Security Server version 12.76. This document explains how to configure the Guest and the Host for RADIUS authentication, with the authentication flows supported in version 11.6, and extended in versions 12.71 and 12.76. **Pre-requisites** Â Â LDAP and RADIUS servers are already setup Â Â NRC components (Guest, Host and Netop Security Server) and licenses Â

Posted - Fri, Jul 25, 2014 2:28 PM.
Online URL:
https://kb.netop.com/article/netop-remote-control-multi-factor-authentication-using-radius-370.html