Active Directory Remote Authentication Implementation Guide

IT Administrator

Document Details

Document #: 160_SG640_190823

Release Version: 06.40.00.00

Version Release Date: March 2019

Overview

Audience: The Active Directory Administrator of CrunchTime's on-premise client.

This document explains how to implement Active Directory Remote Authentication for IT.

System Requirements

- CES Release Version 06.40.00 or higher
- Be sure to grab the latest version of this document here: https://links.crunchtime.com/SG-ADRemoteAuthIT

Other Related Documentation

- AD Remote Sync Guide - IT: https://links.crunchtime.com/SG-ADRemoteSyncIT
- AD Remote Auth Guide - Apps: https://links.crunchtime.com/SG-ADRemoteAuthApps
- AD Remote Sync Guide - Apps: https://links.crunchtime.com/SG-ADRemoteSyncApps
- AD Remote Sync Guide - CT Admin: https://links.crunchtime.com/SG-ADRemoteSyncCTadmin

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Implementation Steps

1. Create a service account in the Active Directory that is a domain account with read-only access to all Active Directory users.

2. Provide the following Active Directory information to the CrunchTime Application Operator.
   - **remote.directory.url**: LDAP connection URL. Typically in the form of *ldap(s)://ip.address/dc=xxx,dc=local*
   - **remote.directory.domain_name**: Active Directory domain name, typically in the form of *orgname.local*
   - **remote.directory.search_base**: Highest Organizational Unit in Active Directory that CrunchTime Application is allowed to search users in. It can be as high as the root of the Active Directory. A typical value is *ldap://ip.address/OU=top_search_ou,DC=xxx,DC=local*
   - **remote.directory.search.follow_referral**: *false* if you only have one domain; *true* if you have multiple domains joined in a Forest and want to search for cross-domain membership
   - **remote.directory.sync_user.name**: Name of the service account created in Step 1
   - **remote.directory.sync_user.pass**: The password for the service account created in Step 1

3. Make Active Directory server accessible to CrunchTime Applications
   - If using LDAP protocol, open port 389 for connection
   - If using LDAPS protocol:
     - Whitelist IPs of CrunchTime Applications; Blacklist others in firewall
     - Open port 636 for connection
     - Complete the “Certificate” step below

4. Certificate for LDAPS (if using)
   - Use SHA-256 to create the certificate; SHA-1 is not supported
   - When creating the certificate, be sure to have IPAddress of the Active Directory server listed in the content of “subject alternative name” of the certificate.
     (Reference: *https://stackoverflow.com/questions/29157861/java-certificateexception-no-subject-alternative-names-matching-ip-address)*
   - Make sure the certificate is on the Active Directory server
   - Provide this certificate to the CrunchTime Application Operator

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com