RAPTOR®
TECHNOLOGIES
THE GOLD STANDARD IN SCHOOL SAFETY

Enterprise Identity Management

Frequently Asked Questions

Q 1. What is Enterprise Identity Management?

Enterprise Identity Management provides a single point for application authentication and authorization to ensure authorized personnel in a school or district have the appropriate access to technology resources.

Q 2. What is "Active Directory"?

Active Directory (AD) is a core component of Microsoft's implementation of an Enterprise Identity Management System. AD functions as an identity provider (IDP) offering user authentication and authorization to applications and services.

Q 3. Does the Raptor system integrate with Microsoft Active Directory?

Beta testing is currently underway. The integration is expected to be released during the 2019-2020 school year.

Q 4. What are the benefits of using AD with the Raptor system?

1. Single point of authentication - There is no need to create Raptor user accounts because AD controls both the user's authentication and their role within the Raptor system.
2. Leverages your existing AD credentials - Users can now use their AD credentials to access the Raptor system, alleviating the need to remember another username and password.

Q 5. If an employee leaves, do I need to do anything in the Raptor system, or is disabling their AD user account sufficient?

Disabling a user's account in AD automatically disables their access to the Raptor system.

Q 6. Can I provide access to the Raptor system to users I don't manage in my AD?

Yes, the Raptor system authenticates users that are not available in AD.

Q 7. Can I control the role of a Raptor user from within AD?

Yes. As part of the AD configuration, Raptor security groups (which map to Raptor roles) are associated to those persons defined in AD that need access to the Raptor system.

Q 8. Do I need to do anything to my existing Raptor user accounts when integrating with AD?

No. When the Raptor user logs in, their user account in the Raptor system automatically converts to AD-controlled.

Q 9. What does it mean when a Raptor user account is AD-controlled?

AD-controlled Raptor user accounts contain fields that cannot be updated (e.g. user's first name, last name, and role). Fields associated with managing the user's passwords are not displayed as password management takes place in AD rather than Raptor.

Q 10. Do you support secure access markup language (SAML)?

Yes, we support SAML with the release of 6.1.8.

Q 11. Does the Raptor system support active directory federated services (ADFS)?

Yes, we support the SAML protocol which can communicate with ADFS.

Q 12. Do you support Open Authorization (OAuth)?

Yes, we support OAuth.

Q 13. Do you support Google G-Suite?

Yes, we support authentication using Google G-Suite.

Q 14. Do you support LDAP?

Unfortunately, not at this time. However, we may add LDAP integration in a future release.

Q 15. Is there a cost associated to integrate with AD?

As an enterprise-level software solution provider, Raptor includes Active Directory integration with your subscription at no additional cost.

Q 16. How do I get the Raptor system integrated to my AD server?

We are currently testing the integration. Simply contact your client services manager or Raptor at 877-772-7867 for additional information on the AD integration. For support questions, dial 877-772-7867 extension 2.